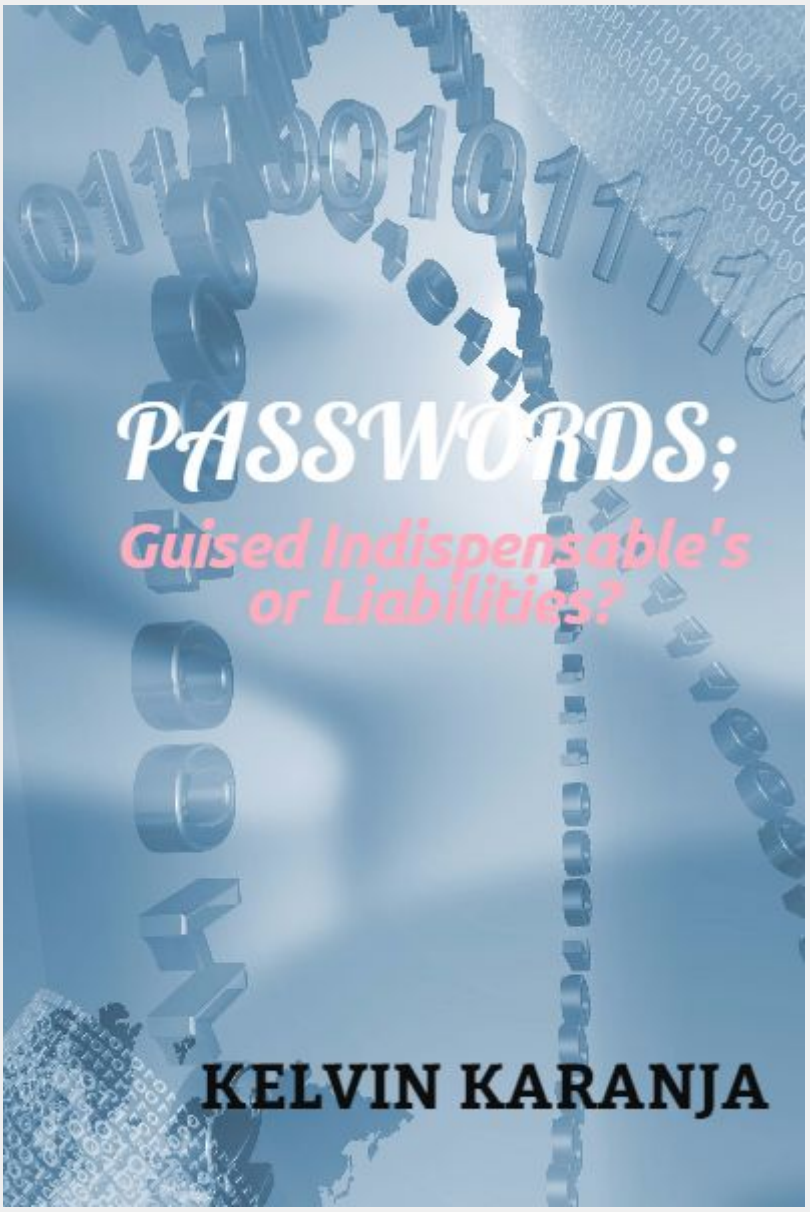


CONTENTS

Chapter 1:The Password.....4
Introduction.....4
Why Use a Password?.....6
The Password Security Mechanisms.....8
Password Policy.....8
Aspects of Password Policy.....10
Storage of Passwords.....13
Authentication of Passwords.....18
Application of PAKE.....20
Emails and Passwords.....20
Areas Where Emails can be Compromised.....21
One Time Passwords (OTPs).....22
Approaches to OTP Generation.....24

Methods of OTP Delivery.....25
Shortcomings of OTPs.....26
Challenges Facing Two-Factor Authentication.....27
Usernames and Email Addresses.....31

Chapter 2:Common Selection Criteria.....32
Human Generated Passwords.....33
Weaknesses of Human Generated Passwords.....34
Keyboard Usability Considerations.....36
Names.....38
Short Passwords.....40
Any Significance of Using Spaces in a password?.....42
Security Questions.....43
Random Things.....45
Mnemonics.....47
Numbers and Symbols.....49
Reusing Passwords.....52
Sharing of Passwords.....53
Mangling/Mirroring it Around.....55
Usernames and Email Addresses.....55

Chapter 3:Cracking Passwords.....56
Cracking Passwords.....56
Dictionary Attack.....58
Rainbow Table.....62
Brute Force.....63
GPU.....63
Hybrid Attack.....64
Encryption and Cryptography.....68
Emails,End-to-End Encryption vs Client Side Encryption in relation to Passwords.....70
Hashing Algorithms.....73
Salts.....74
Password Cracking Tools.....76
Online 'Hacker' Forums.....78
Openwall.com.....80
Anatomies of Password Cracking.....*83*

Chapter 4:Secure Techniques.....87
Password Length and Strength.....90
Reference To Password Blacklists.....91
Careful Capitalization.....91
Random Password Generators.....91
Password Strength Checkers.....92
Password Managers.....95
Types of Password Managers.....97
Password Safe.....99

Best Password Managers.....101
Password Longevity/Duration.....101
Personal Password Policy.....102

Chapter 5:Networks and their Security Flaws.....104
WEP.....104
WPA/WPA2.....106
VPNs.....107
VPN Authentication.....109
Routers.....109
Unencrypted Tunnels.....111
VPNs in Private Networks.....1.11
Limitations of VPNs.....112
Proxy Servers.....113
Configuring Proxy Servers.....114
Setting up Firewalls.....116

Chapter 6:Problems With the Web and Securing it.....118
Storage of Passwords on the Web.....119
Poor Encryption,Hashing and Salting Techniques.....119
Website Hacks.....121
Injection Attacks.....121
Solutions.....129
Poor Password Policies.....132
Solutions.....133
Data Breaches.....134
The Heartbleed bug.....135
Solutions.....137
MitB.....137
Protection against MitB.....139
Phishing.....141
Solutions.....145
Clickjacking.....147
Backdoors.....148
Direct Access Attacks.....150
Eavesdropping.....152
General Solutions.....153
Install and Update Antivirus Software.....153
Methods of Protection from Viruses.....154
Install & Update AntiSpyware and AntiMalware.....155
Update your Operating Systems.....157
Remember Wannacry?.....157
Be Careful what you Download.....158
Turn Off your Computer.....159

Chapter 7:The Future Of Passwords.....159

The Password is Dead.....160
Replacing the Password?.....161
Most Popular Alternatives to Passwords.....162
Project Abacus.....165
Final Thoughts.....166
About the Author.....168

DISCLAIMER

Every attempt has been made to verify the information provided in this ebook.Every effort has been made to ensure the content of the ebook is as complete and accurate as possible.The author shall not be responsible for any errors,inaccuracies or omissions.

Kelvin Karanja © 2017
All Rights Reserved

Follow Tech Bytes at Tech Bytes
& Kelvin Karanja at KevoKaras for more.

1] The Password

Introduction



The password is a phenomenal that has being in existence since the dawn of the web,in fact passphrases were used by ancient societies as a security measure,and this just goes to show the innovative nature of mankind throughout the ages.The password is a mechanism that provides a secure gateway or a loophole to ***CyberSecurity****;whichever way you look at it as there are two sides to a coin(****others say 3****).With the passing of time,it has become easier to compromise passwords and therefore there is no guarantee of security by having a password,it has to be a secure one and the online service you sign up for should also offer an environment that maintains that level of security and even improves the level of security rather than diluting it and making the user's vulnerable.Many of us have been culpable of numerous password flaws which compromises our Cyber Security.The statement 'Do anything and everything and even hire a Cyber Security team but if your password is weak,none of it will matter' says a great deal about the many underlying* ***issues*** *relating to Passwords other than say password length and to an extension the whole Cyber Security Challenges.The aim of this eBook is to try shed some light,understand and resolve most of these issues,because in the words of* ***Calvin Coolidge*** *(****US President****)....'We cannot do everything at once,but we can do something at once'.I believe that we'll definitely have made an important step forward.*

Why Use a Password?



Everyone in the world who is tech savvy has used and interacted with a system that requires him to have and use a password.In fact due to phenomenons such as social networking,passwords have become something of a household name.A password is basically a word or string of characters used for user authentication to prove identity and access a resource or login to an online account.A typical computer user of the 21st Century has a Password(**s**) for various purposes:

I. **Logging Into Accounts**
II. **Retrieving E-mails**
III. **Securing Devices e.g Phones,PCs,Tablets etc**
IV. **Databases**
V. **Websites**
VI. **Networks**

There are many factors which have necessitated the use of the usage of the Password and it is hard to now imagine a world without them.Some of these factors might vary from one user to another,depending on many things-

I. **Privacy and Protection of Private Data(the Main Reason)**

II. **Other Attacks**



Passwords are nonetheless prone to physical security issues;from simple vulnerabilities like bystanders prying at what you're typing,shoulder surfing in crowded workstations to complex threats like video cameras and keyboard sniffers being mounted on your PC to spy on you and try stealing your password,writing your password on a sticky note and placing it on your monitor especially in the workplace is not a good practice either.All of these loopholes should be **sealed** at all costs to maintain the integrity of the Password.

Most computer systems have the option of showing or obscuring(**masking**) using * and • ,as the password is being typed.While,this is good practice other users want to be allowed to chose whether to obscure or not because obscuring will likely lead to stressing the user since he will not clearly see what he is typing which could result to selection of weak Passwords to avoid such struggle and stress.Weighing in on this issue,I believe that its better that the user is provided with the option of obscuring the password or not,depending on the preferences of the user.However,the user should exercise caution when doing this to ensure he does not fall prey to Physical Security Threats.



Password Security Mechanisms

This is how computer systems have being designed to ensure that the passwords employed by the user,do serve their purpose which is providing security and that this is done in a manner that leaves little or no room for vulnerabilities.Some of these may fall into the bracket of **Password Policy**(**see chapter 4**).Most Computer systems are structured to do the following:

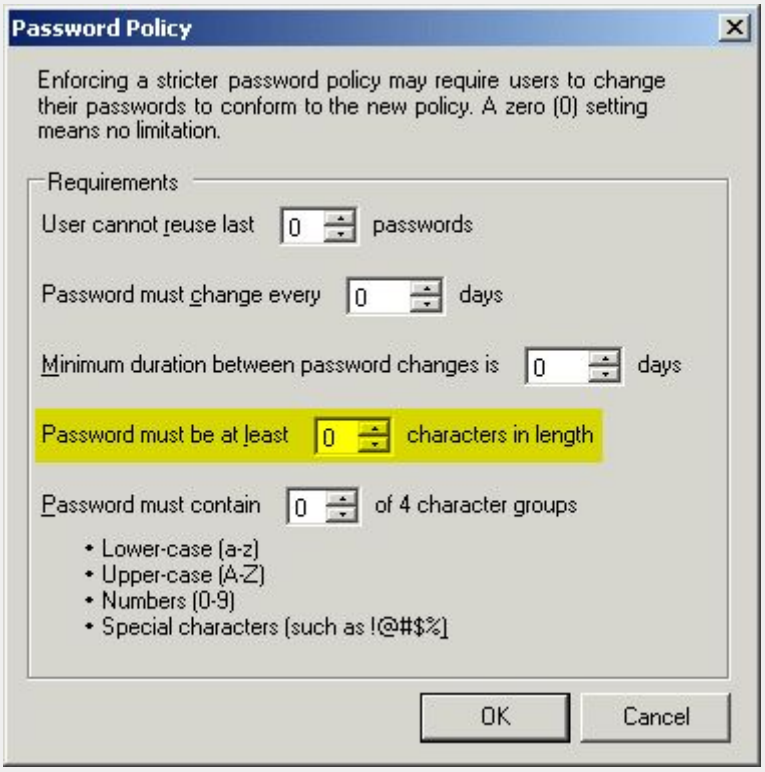
I. **Not displaying the password on the display screen as it is being typed.Often times obscuring or masking it using bullets(•) and asterisks(*).**
II. **Allowing passwords of adequate length.**
III. **Using two-factor authentication; such as sending a text message, an email or alert via a third-party app whenever a login attempt is made.**
IV. **Requiring characters from various character classes in a password such as "having at least one uppercase letter and also at least one number" Etc.**

However,despite having such measures aiming at providing an optimal level of security in place,some measures are considered by users as being too stringent and thus people tend to treat them with hostility and drag their feet at abiding by them and in the long run;the security level will have decreased.

Password Policy



A password policy is a set of rules or measures designed to ensure strong passwords are selected and used properly.The policy may apply to an institution or company.The **main** goal is to enhance computer security.The best password policy is one that helps users in creating secure passwords rather than try to strongarm and force users to do so.Using Technology and policy to make passwords stronger and secure might not necessary be enough because the weakest element in the system is the human element;some security players have even suggested that it would be better to do away with the human element by generating random passwords.However,although this is in theory a very good idea,practically it is impossible to completely do away with the human element even if you generate random passwords.You can sideline human beings from the generation but not from the use of these passwords;which generates other challenges.Selecting good passwords requires education;for both users and system administrators so that they can be able to educate and help the users.Complex Password requirements have usually been proven to be off-putting and according to many reports,over half of users queried abandon creation of online accounts,another around 55% **abandon a login page** because they have forgotten a password or incorrectly answered a security question.

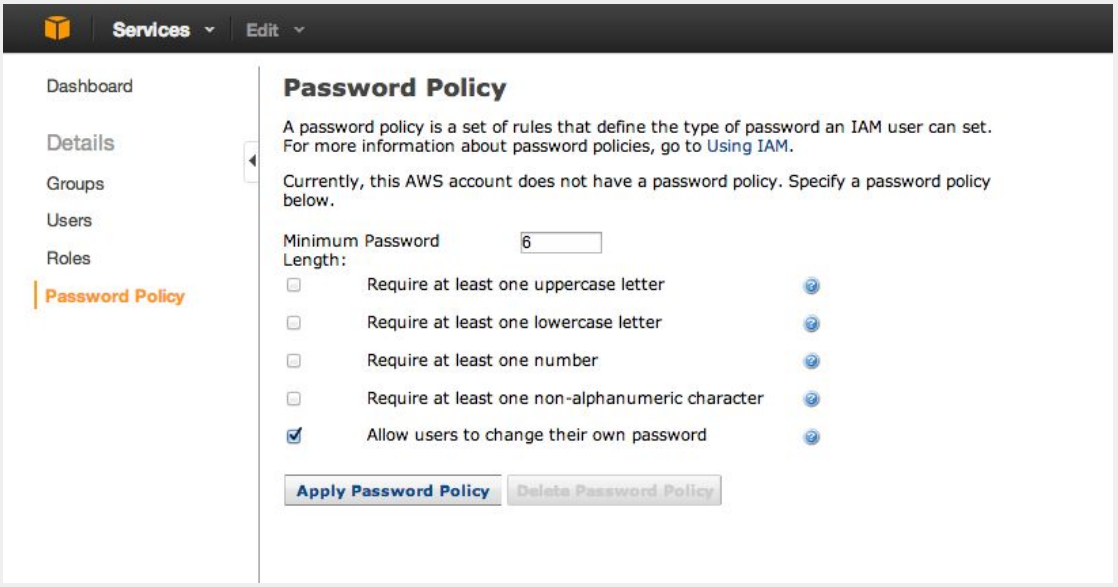


Aspects of Password Policy

The aspects of password policies may vary from organization to organization depending on their threat assessment of possible vulnerabilities;irrespective of these differences the bottom line is **security** to the firm,its resources and the users.

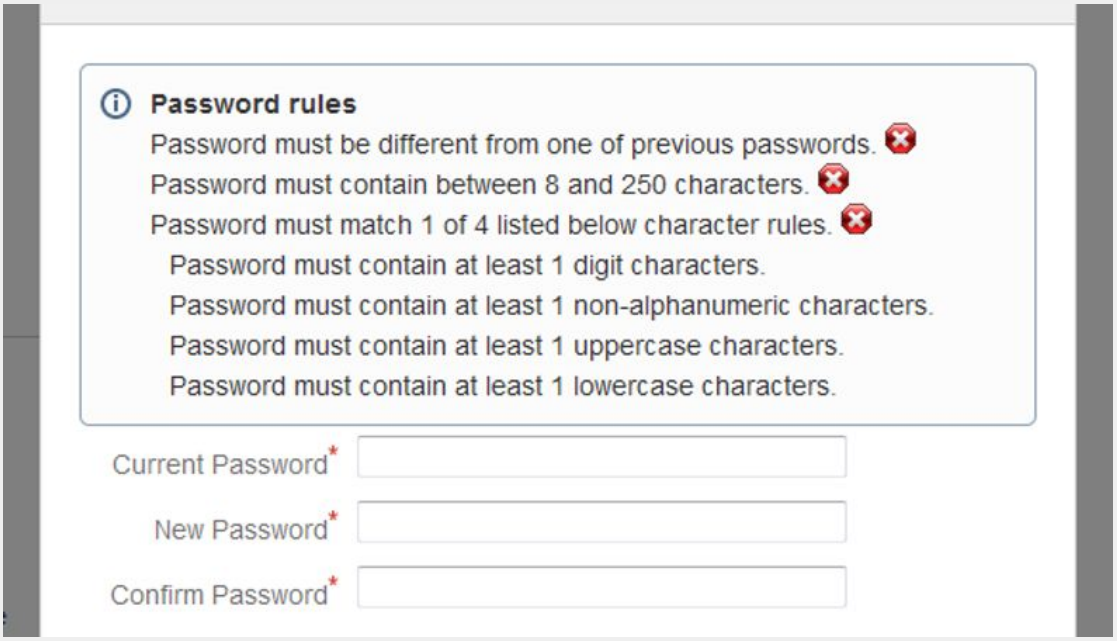


There are many things that a password policy ought to do;It should Assist users to choose strong passwords,prescribe the constitution of characters which passwords must contain,ensure the passwords are suited to the target users,provide recommendations for users with regard to the handling of their passwords,prompting users to change passwords which have been lost or compromised and ensuring that passwords don't last beyond a certain period of time among things.To achieve such goals it is important that a good password policy has a training program where users are trained on the basics of **password selection** and also train those who face challenges (**lost passwords**) or fail to follow the password policy(**inadequate passwords**),Rewarding users of strong passwords by reducing the rate of password change(to an extent asking users to change strong passwords is not a very wise thing to do because they may end up selecting a weaker password than the previous one).

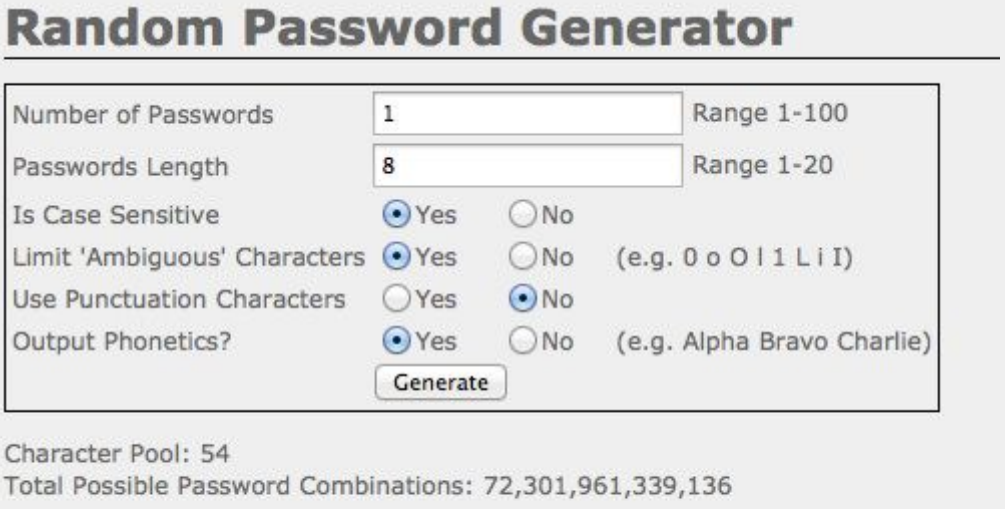


1)Length and Details/Constitution

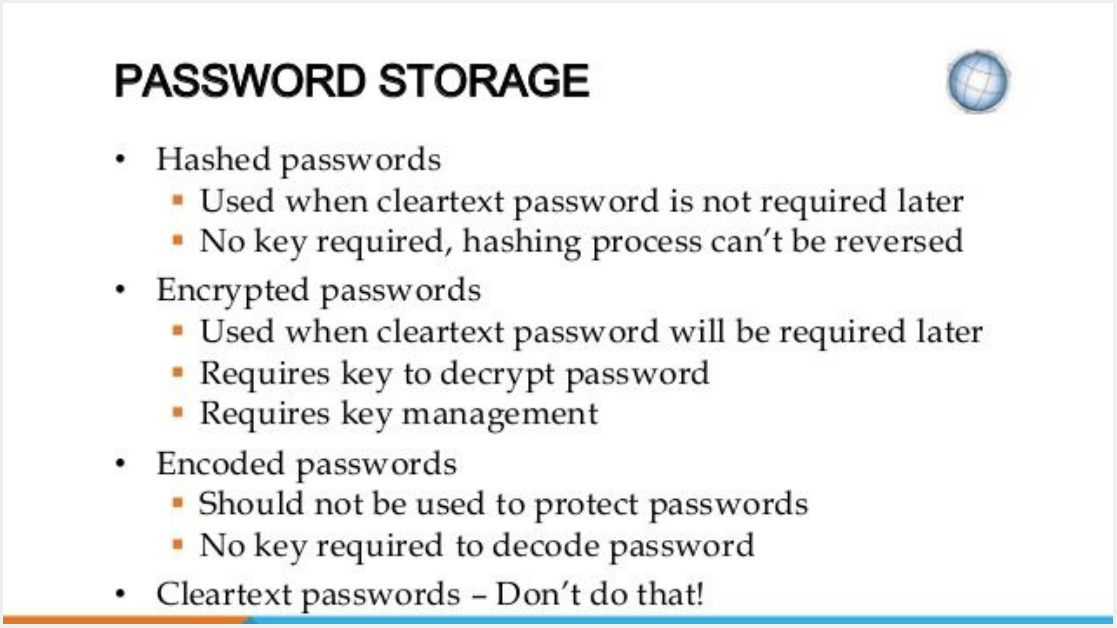
I. **A minimum password length of 8 characters**
II. **Prohibition of words found in a password blacklist**
III. **Case Sensitivity - using of both uppercase and lower-case letters.**
IV. **Prohibition of words found in the user's personal information (e.g social media bio,statuses,profiles etc)**
V. **Prohibition of use of Company Name or an Abbreviation (Mnemonics)**
VI. **Inclusion of Special Symbols/Characters such as #,$,@**
VII. **Prohibition of passwords that match the format of mobile/telephone numbers,calendar dates,license plate numbers or other common numbers.**
VIII. **Reference to blacklists and using blacklists to block common,weak and easily guessed passwords.**
IX. **Password Expiration- The password becomes inactive after a certain period of time.**



2)Random Generators - Here,the user will not come up with the password but systems following a certain set criteria(of a password policy) create the password for him.The Random Generators could also let the user to select a password from a limited number of choices.

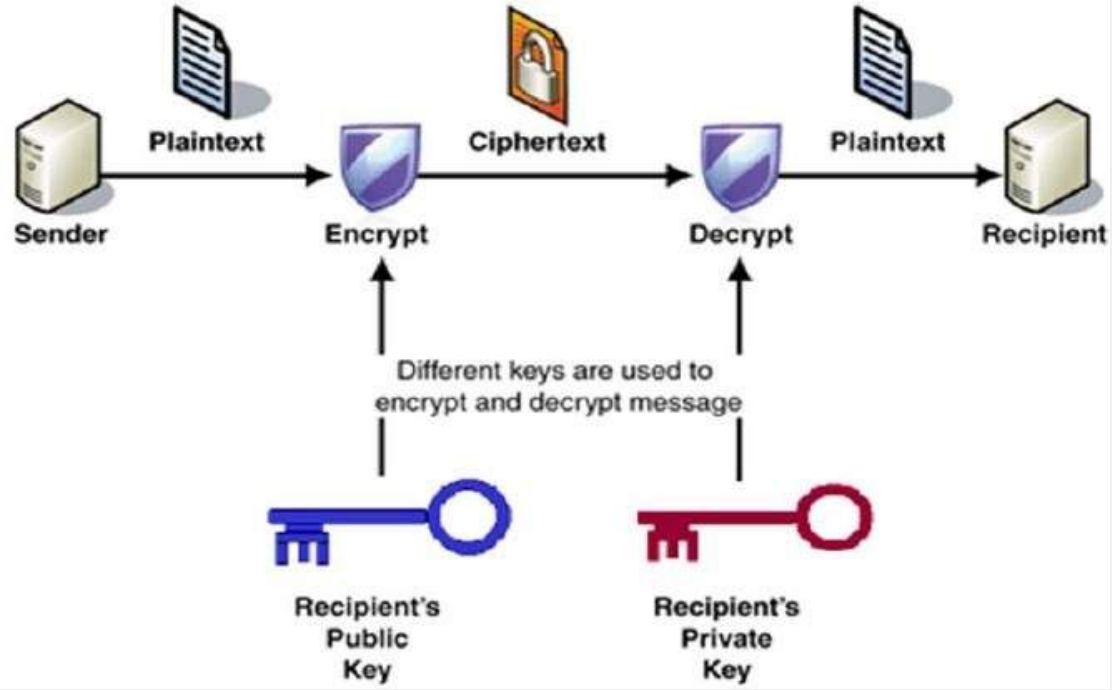


Storage Of Passwords



Back in the early infancy stages of Computer Science,websites stored user passwords as **plain text**.Password cracking was not as big as it is today,the protection and security mechanisms were also designed to deal with such lower-level threats.In order to verify that the user sent in the correct password a copy of the passwords were stored in a file somewhere, and was used to check the user's submitted password against the list.As time went by,attackers devised methods of accessing the database files(Through Deception like politely asking for permission to access such files)that had passwords.The security players needed to do something different,and quickly.Fast forward some time later,Hashing was born.A hash function is a piece of code that takes a piece of information and scrambles it up mathematically into a fixed-length piece of gibberish.This is called 'hashing' the data.What's so cool and unique about them is that **they only go in one direction;they are irreversible**.It's fairly easy to take a piece of information and figure out its unique hash but quite tasking to take a hash and find a piece of information that generates it.An attacker,can use commercially available tools to have a go at guessing the Passwords.Such tools work by hashing possible passwords and comparing the result of each guess to actual password hashes.If a match pops up they definitely know that their guess is the actual password.Hashes have some really useful properties for password applications.Now,instead of storing the password,you store the hashes of the passwords.When you want to verify a password,you hash it, delete the original, and check it against the list of hashes.Hash functions all deliver the same results, so you can still verify they submitted the correct passwords.Crucially,the actual plaintext passwords are never stored on the server.So,when hackers breach the server,they can't steal any passwords – only hashes.The hackers response to this was to spend a lot of time and come up with really clever ways to reverse hashes.There are various forms in which Passwords on a computer system can be stored.Oftentimes they are stored as plaintext,against which to compare user log on attempts.These ones are not secure since if an attacker gains access to such an internal password store,all passwords and by obviously all user

accounts will be compromised.In fact storing passwords as plaintext is one of the biggest mistakes any online service can ever make.



Cryptanalysis is a science of data encryption and is mostly used by computer scientists and cryptanalysts to recover Passwords from data that have been stored in or transmitted by a computer system.Therefore,more secure computer systems store each password in a cryptographically protected form making it a tall order for someone who gains internal access to the system getting the password,whilst still leaving room for user validation.Other computer systems have gone a notch higher and don't store passwords at all,which is quite good.They store one-way derivation like an advanced hash or a polynomial modulus.(The salt must be saved for each user and is usually stored beside the username and password hash, so the information is available during each user login.Salt is rarely kept apart from the hash.Even when known,its virtue lies in its uniqueness,which defeats pre-computation of results.)

Cryptanalysis is the science and study of methods for breaking encryption schemes. A cryptographic system is said to be **breakable** if plaintext can be obtained from ciphertext without knowing the key, or if the key can be deduced from observed ciphertexts and corresponding plaintext information. There are three main lines of attack:

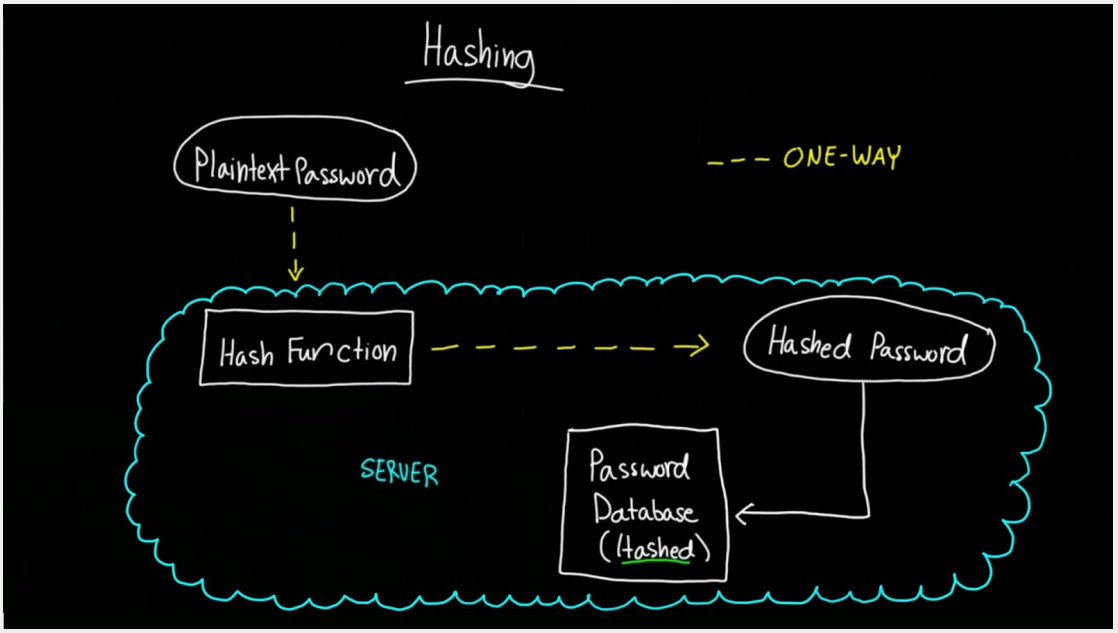
- **Ciphertext-only attack**. The cryptanalyst has several pieces of ciphertext that were all encrypted using the same encryption algorithm. The goal is to recover as many plaintexts as possible or, better yet, to deduce the key(s) used for encryption and/or decryption.
- **Known-plaintext attack**. The cryptanalyst is able to obtain several plaintext-ciphertext pairs. The goal is to deduce the key(s) used for encryption and/or decryption, so that any further messages encrypted with the same key(s) can be decrypted.
- **Chosen-plaintext attack**. The cryptanalyst can choose plaintexts and obtain the corresponding ciphertexts. The goal is to choose the plaintexts such that the resulting plaintext-ciphertext pairs make it as easy as possible to deduce the encryption and/or decryption key(s).

User details are stored in the following way and usually separated from each other using colons:
1)The Username(on the left)
2)The Number Identifier of the hashing algorithm used (on the right after the colon)
3)The Salt(after the Hashing algorithm number identifier)
4)The very long hash
5)Details about when the password was last modified,how old it is,when the account will expire among other details.

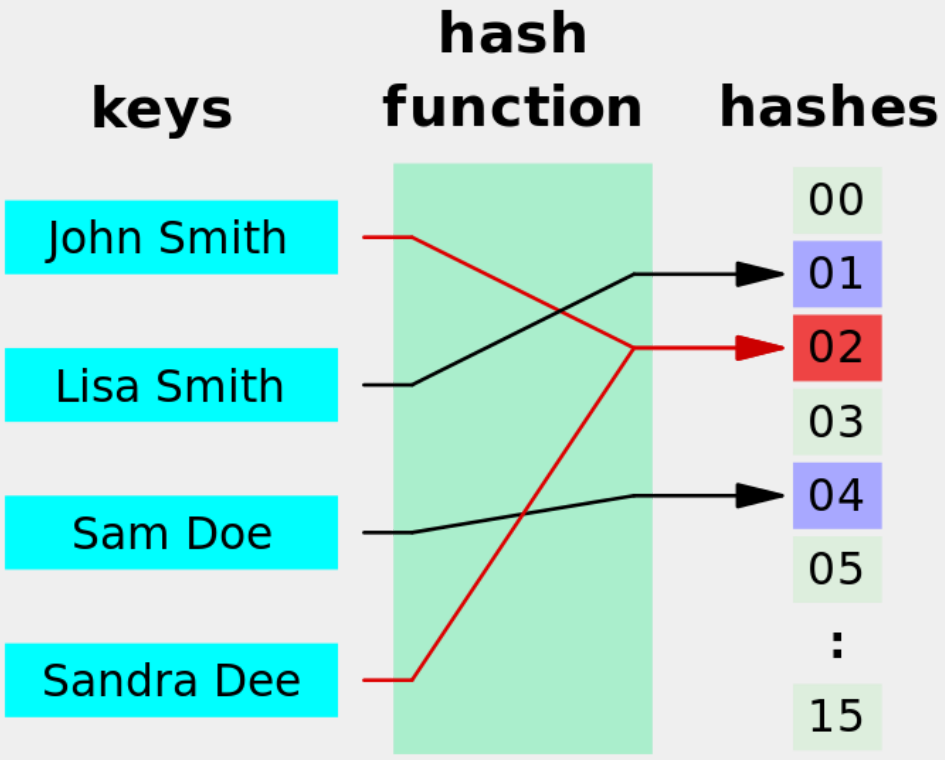
Example of a Stored Password:

testuser:$6$2lvEhpi5$KnVn901C4Y23zsVZK1/UILbTkKIU6hA6V/0pXZ3yQU.EhVxQS6/KjaO2bH7VZOOr/DTGko9LjqWOi7CrU.Ggy0:15569:0:99999:7:::

The line is broken up by colons—first comes the username,then the lengthy password section,then data about when the password was last changed,how old it is,when the account expires,and more.



Hash- Hashing is the transformation of a string of characters into a usually shorter-fixed length value or key that represents the original string.Roger Needham is credited for inventing the common approach of storing only a hashed form of the plaintext Password.This system allows the user to type in a Password on such a system,the password handling software then runs through a cryptographic hash algorithm,and if the hash value generated from the user's entry matches the hash stored in the password database, the user is then permitted access.The hash value is created by applying a cryptographic hash function to a string consisting of the submitted password and,in many implementations,another value known as a salt.A salt prevents attackers from easily building a list of hash value or simply guessing them.Main storage methods for passwords are text,hashed and salted and reverse encryption.If an attacker gains access to the Password file,it is stored as a plain text and no much work for him such as cracking is necessary because its plain text and the password is crystal clear.If it is hashed but not salted,then it is vulnerable to rainbow table attacks(**more efficient than Cracking**).If it is reversibly encrypted,the attacker needs only get the decryption key and the file...If he does get them,nothing can save you now because,no cracking is necessary.However,if he fails to get the key cracking is not possible.

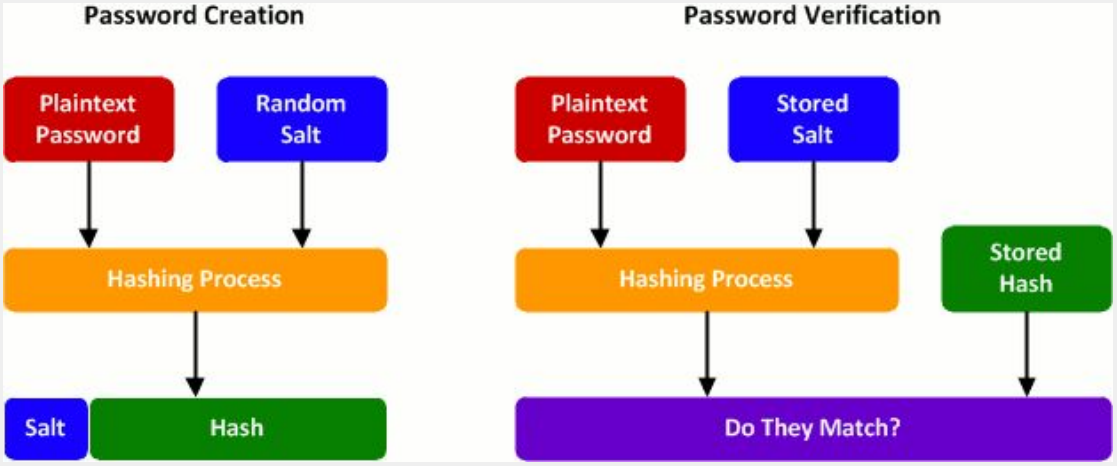


Rainbow Table Attacks- A precomputed table for reversing cryptographic hash functions,usually for cracking password hashes.Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters.

An attacker,can use available tools-commercially available ones to have a go at guessing the Passwords.Such tools work by hashing possible passwords and comparing the result of each guess to actual password hashes.If a match pops up the definitely know that their guess is the actual password.

Authentication of Passwords

When logging into your online account and you type your password,how is the password retrieved from the server and verified? There are a few methods such as Cryptographic Protection which uses Transport Layer Security (**TLS**),previously known as **SSL**.It is a feature built into browsers and the TSL/SSL feature is shown by a closed lock icon displayed at the beginning of the address bar(top left).Another mode of verification is the hash-based method;A client ought to prove to a Server that they know what the shared secret(the password) is and the Server then has to obtain the shared secret from its stored form.The shared secret during remote authentication in most Operating Systems like **Unix-type** systems is the Hashed form;in case of attack,the attacker will only need the hash rather than the original password to authenticate.



In a zero-knowledge password proof,neither the password or it's hash are transmitted. As the name suggests;the system proves knowledge of the password without exposing it.

An Augmented system allows a client to prove knowledge of the password to a Server,and the server only knows a hashed password.To ensure that in case the attacker infiltrates the system he won't compromise the password,the unhashed password is the one that is actually required to gain access.An Augmented System for password-authenticated key agreement such as SRP-6 and B-SPEKE among others avoid the limitations of hash-based methods,because hash-based methods require a client to prove to a server that they know what the shared secret(password) is and the server then has to obtain the shared from its stored form.

Password Authenticated Key Agreement (PAKE) is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password.One of its secure properties is that a Man-In-The-Middle or eavesdropper cannot obtain enough information to be able to **brute-force guess** a password without further interactions with the parties for each (**few guesses**)...to an extent therefore, strong security can be obtained using weak passwords.A Cryptographic key is established using an exchange of messages,making sure that an unauthorized party(like one who is in control of the communication channel but doesn't possess the password) is not a participant in the method and has very little chance of successfully brute-forcing the Password.PAKE comes in two forms;Balanced and Augmented Methods.

Password Authenticated Key Agreement entails the following methods:
I)Balanced Password Authenticated Key Exchange
II)Multi-party and Multi-server methods
III)Augmented Password Authenticated Key Exchange
IV)Password Authenticated Key Retrieval
In the most stringent password-only security models;there is no requirement for the user of the method to remember any secret or public data other than the password.

Balanced PAKE-Allows parties that use the same password to negotiate and authenticate a shared key.Therefore,both parties have either password,or in certain cases a private key for corresponding public key.PKI can be represented by ephermal keys to simplify key exchange whilst requiring less user interaction for Public Key Management.Examples:

I)Encrypted Key Exchange (EKE)
II)SPEKE(Simple Password Exponential Key Exchange)
III)PAK and PPK
IV)Dragonfly-IEEE std 802.11
V)SPAKE 1 and SPAKE 2
VI)J-PAKE(Password Authenticated Key Exchange by Juggling).

Balanced PAKE effectively ensure that parties can use the same password to negotiate and authenticate a shared key;therefore both parties either have a password or a private key for the corresponding public key.Examples are:

I)AMP
II)Augmented-EKE
III)B-SPEKE and W-SPEKE
IV)PAK-Z
V)SRP(Secure Remote Protocol)
VI)Aug PAKE

Application of PAKE

1)To ensure that there is a safe matching of the public key,so long as the attacker has control of the active data link between the parties.
2)Implementation of high-entropy cryptographic strong key using low-entropy passwords for authentication.

Emails and Passwords



Email is sometimes used to distribute passwords,but this is an insecure method.If you sign up for an online service for the first time or reset the password,the new password will sometimes be sent via email and since most email is sent as plaintext;a message containing a password is readable without effort during transport by any eavesdropper even if stored as plaintext on the server,an attacker can therefore retrieve it.The message is stored as plaintext both on the sender's and recipient's computers,it is worth noting that only the message contents and attachments are encrypted but the header information such as your address,the recipient's address,subject,date etc thus an attacker on the network (**discussed later in detail**) can be aware of the likely contents and follow the trail of communication and eventually retrieve the

plaintext message from backup,cache and history files of the computer system,if he gains access since such data is usually copied in such directories and locations.



Areas Where Emails Can Be Compromised

Email in general,even when used to communicate over the internet,is unfortunately not that secure because Email was not **designed** with any privacy or security in mind;you need to trust who you email.The biggest challenge is the channel of transmission especially networks which is quite vulnerable.Vulnerable areas:

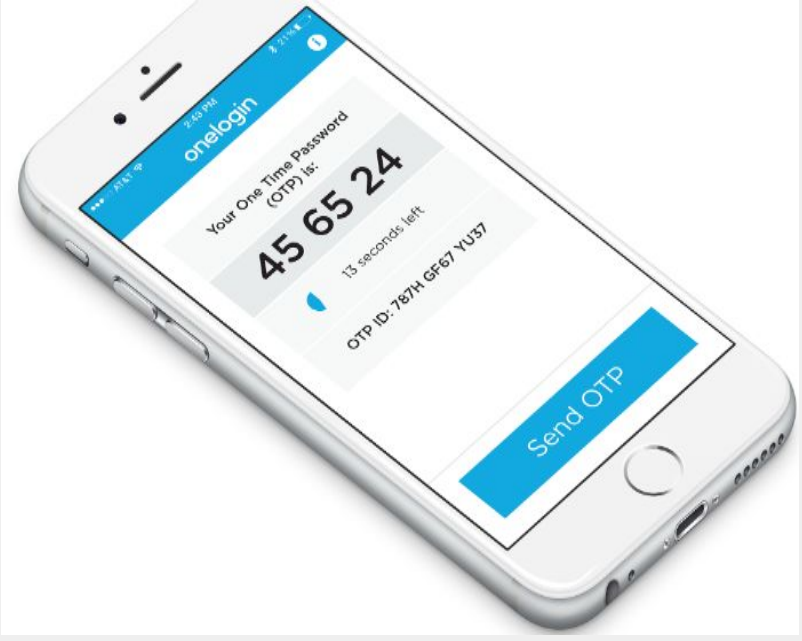
1)**On your Device**
2)**On the Networks**
3)**On the Server(s)**
4)**On your Recipient's Device (s)**



The Network is the most problematic area.The Network connection areas are:
1)Your Connection to your Email Provider(Google,ISP,Outlook,Yahoo,Apple etc)
2)Any Network connections between your email provider and your recipient
3)Your Recipient's Networking Connection to the Email provider.1

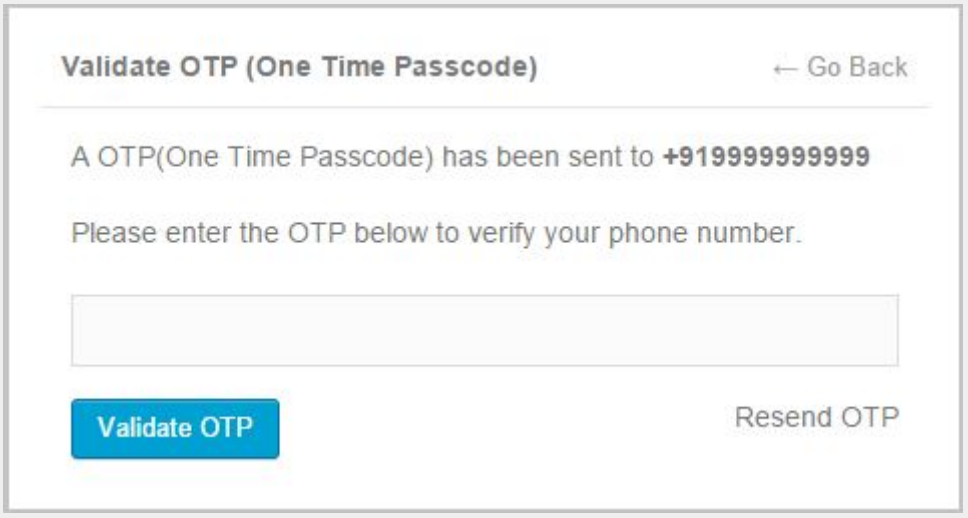
Another shortcoming is that Encryption technology cannot easily and safely used on a smartphone, this is because copying the private keys to a smartphone could be a security risk; thus many people avoid mixing phone and email encryption tools.**Comprehensive encryption**(bearing in mind the shortcomings and place of End-to-End Encryption) could be a big remedy because Client-Side Encryption will only protect transmission from the mail handling system server to the client machine.

One Time Passwords(OTP's)



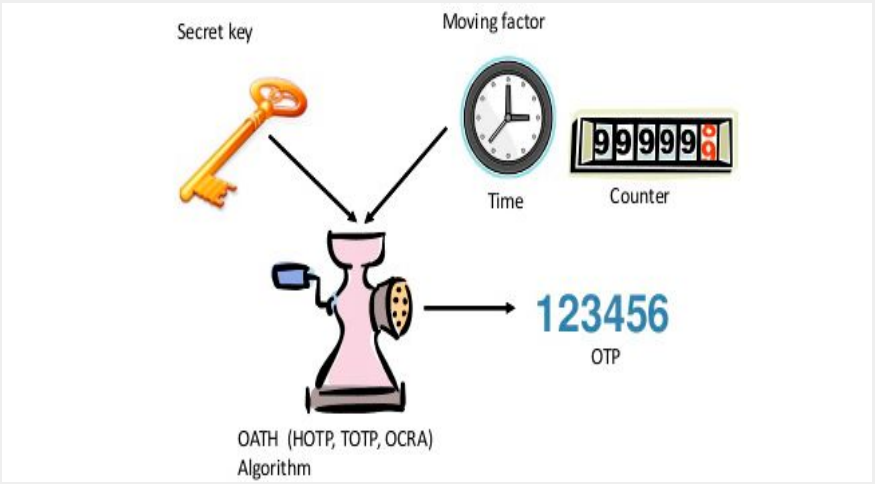
OTPs are passwords valid for only one login session or transaction,on a computer system or other digital device.They have being mainly used(and successfully for that matter) in online

banking.Their huge success can be attributed to incorporating two-factor(or **two-step**) authentication whereby they use something the user has e.g a phone where they send a text message with the OTP to be used with a PIN that only the user knows.Therefore,the user will be aware of any attempt to impersonate him at all times and thus criminal activities can largely mitigated.



OTP generation algorithms make use of pseudo randomness or randomness by making prediction of successor OTPs a harder but to crack.Hash functions are also used and since the resulting value cannot be reversed,it is difficult for the attacker to obtain the initial data before it was hashed;this part is significant because it makes it thwarts the likelihood of predicting future OTPs by observing previous ones.

Approaches To OTP Generation

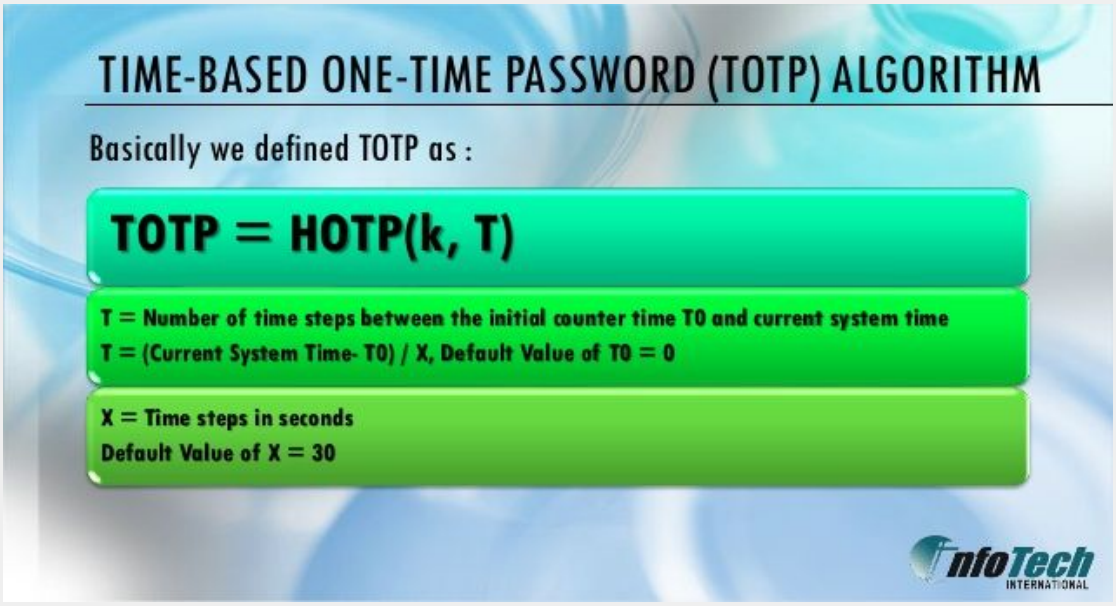


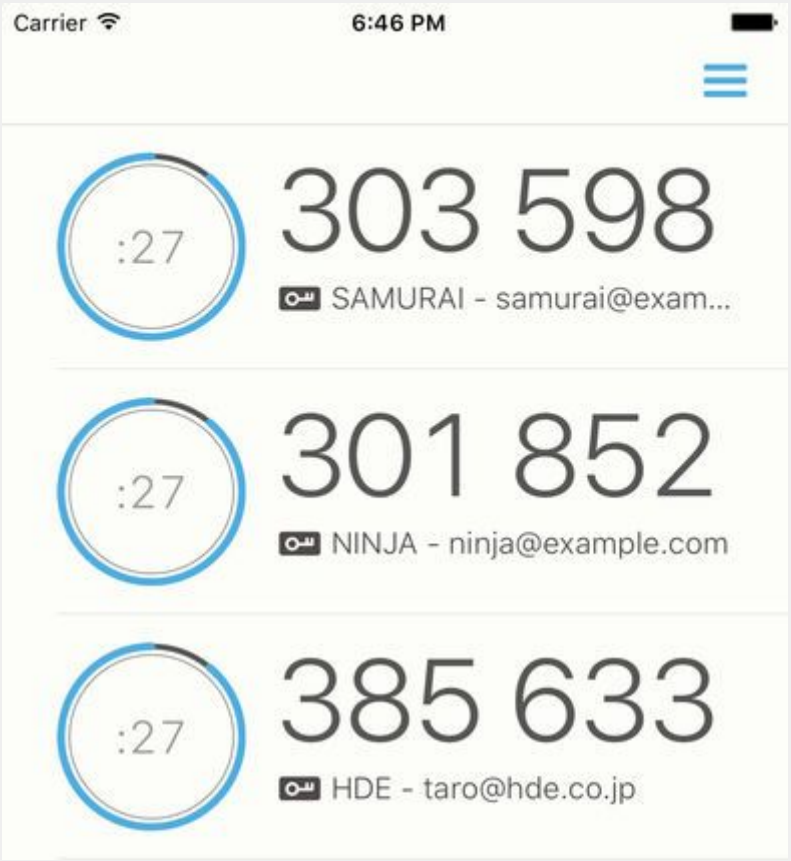
(1)Time-Synchronisation based- The authentication server

and client providing the password work in tandem to make the OTPs validity only last for a short period of time.

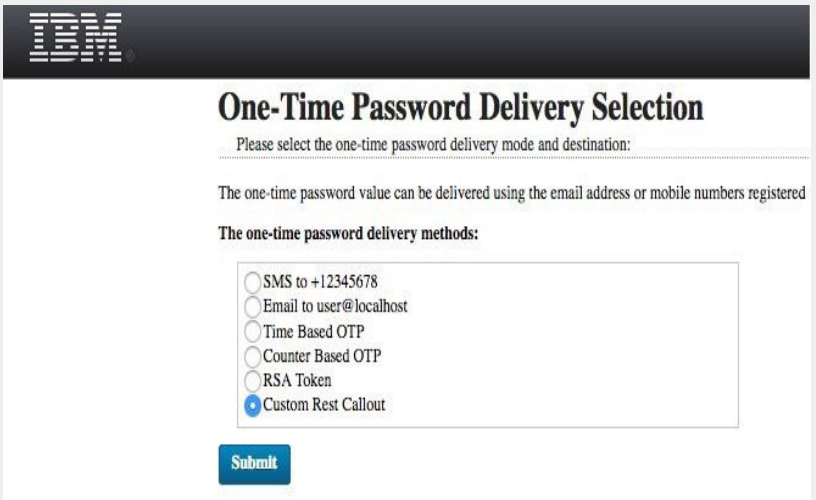
(2)Mathematical Algorithm- OTPs are a chain and are used in a predefined order.The next password to be generated is based on the preceding password.

(3)Mathematical Algorithm- The new password is based on a challenge (using a time-counter or a random number chosen by the authentication server or even the transaction details involved).





Methods Of OTP Delivery



1)Via Text Message-SMS(Most used method)

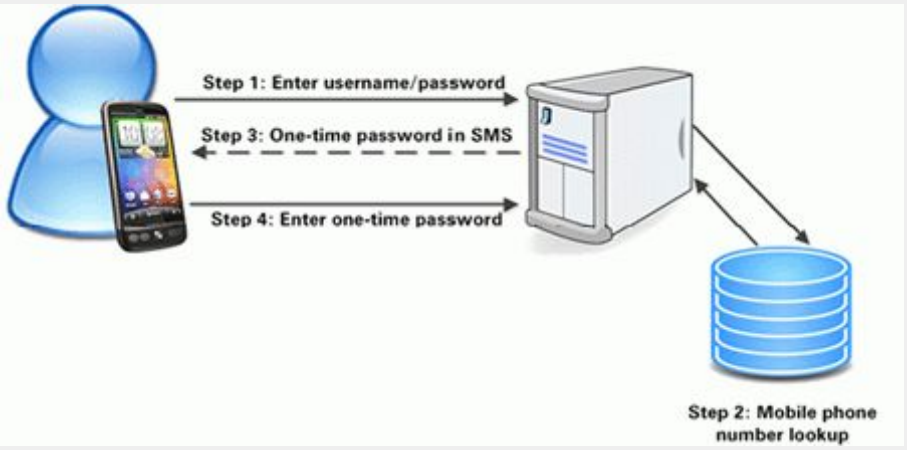
2)Through Mobile Phones (Calls)

3)Proprietary Tokens- Small electronic devices that are manufactured and owned by private companies.They are powered by batteries.Examples are RSS SecureID or HID

Global. 

4)Hardcopy- There are banks which send OTPs printed on paper for Online banking or on Plastic Cards obscured by a layer that the user will have to scratch in order to reveal the OTP.

5)Web based Methods - When a user is registering on a website,he has to choose a select category of things;cars,flowers,dogs,and boats etc.By relying on the user's ability to recognize pre-chosen categories from a randomly generated grid of pictures;the user is at each time of logging in to the site presented with a randomly generated grid of pic alphanumeric characters overlaid on the pictures and is required to look for the pictures that fit their pre-chosen categories and then enter the associated alphanumeric characters to form an One Time access code.



Shortcomings of OTPs

As with everything, there is the good and the bad side.The most used method of transmitting OTPs is through text messages which are themselves faced with a myriad of vulnerabilities but the most prevalent ones on the side of OTPs are Phishing and Social Engineering.Sometimes the batteries of the proprietary tokens may be dead and this makes it impossible for the user to access OTPs.

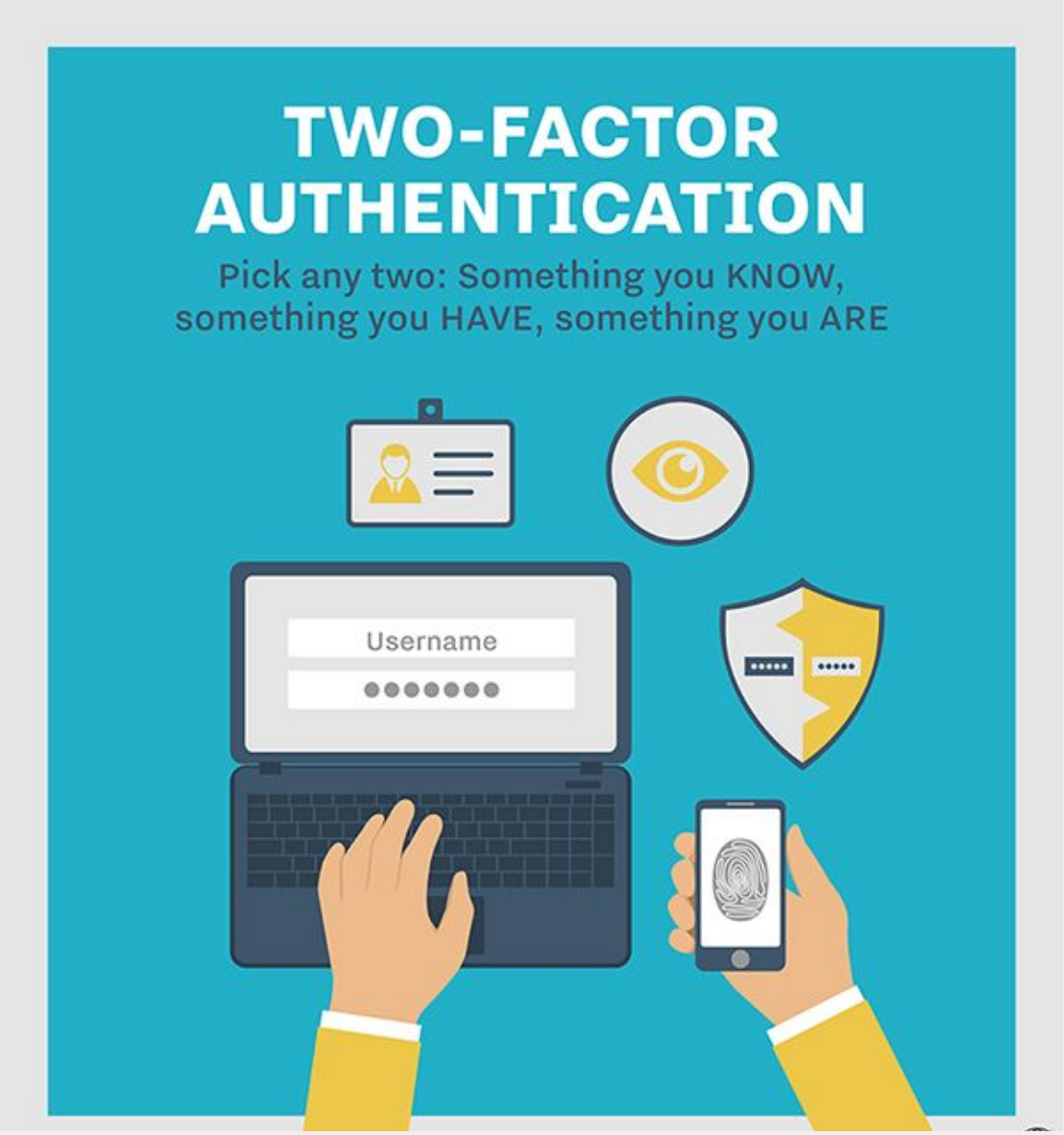
1)Phishing- Attackers will masquerade as let say a bank and ask the user to enter OTPs that they have previously already used.He will use the hashchain to try and predict future OTPs.Pseudorandom (not fully random) generated codes are

most vulnerable to this exploit than truly random generated codes because there is a huge chance of succeeding in predicting the future pseudorandom codes if you look at the past codes.



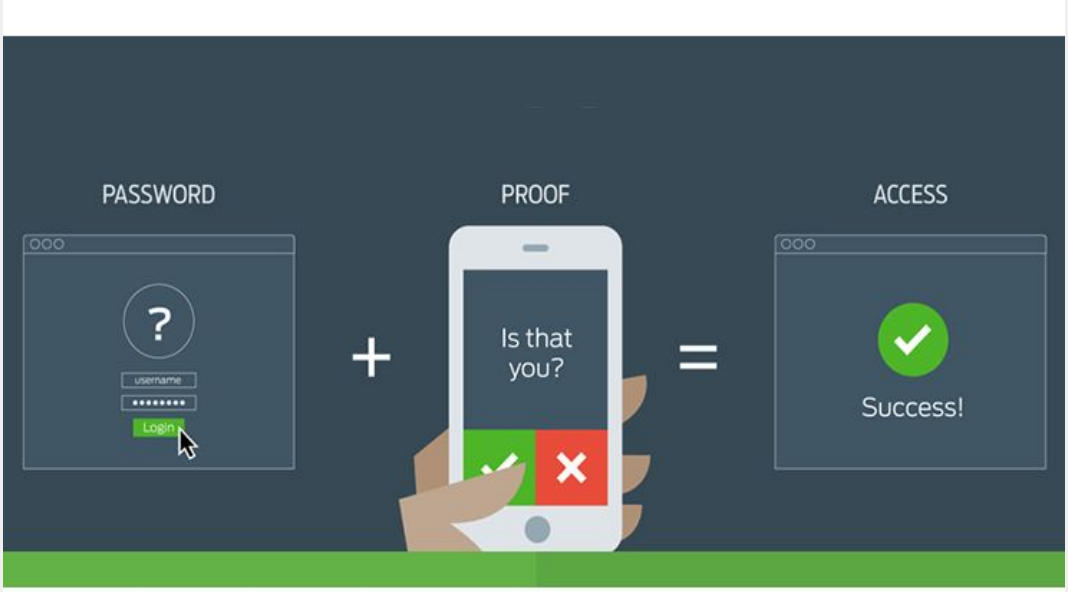
OTPs avoid the shortcomings of the traditional static passwords,with the main advantage being that they are not vulnerable to replay attacks.Users of OTPs should be careful not to fall prey to Man-in-the-middle attacks(**via the networks**).The other main challenge facing them is that they are difficult for human beings to memorize,requiring additional technology to work(I think they offer a lot of security and we can work out a way to bypass the challenges;its only a small price to pay for the enormous convenience they bring).OTPs should not be disclosed to other people or third parties and they could be more effective as part of a layered security system and not alone;ensuring that OTPs are always used with a password that is never sent to the user but instead is known and owned by the user.There have being discussions about the possibility of OTPs enhancing or even ultimately replacing the traditional passwords.There are also other more secure techniques being developed to work with OTPs,so OTPs have a lot of potential.

Challenges Facing Two-Factor Authentication



A Two-Step/Two-Factor authentication requires a temporary code **generated** and sent to something the user has such as a phone or a third-party app for use in addition to a password.Initially it gave an added layer of security but nowadays with advances in technology,hackers can hijack the SMS with the one-time login codes and if they know the password,easily log in to the user's account.It is possible to socially engineer mobile phone authentication.**Twitter** for example,to a large extent depends on SMS and is vulnerable to this type of attack.**De Ray McKesson**,a **Black Lives Matter Movement Activis**t,had his Twitter account hacked during the 2016-17 **US** Presidential Campaigns.The attackers bypassed Two-Factor authentication by calling **Verizon**(his mobile service provider) and impersonated him requesting the company to redirect his text messages to a different SIM Card...they then used his account to tweet Pro-Donald Trump messages;much to the **shock of many**.There have been cases of accounts being hacked-through bypassing Two-Factor authentication.The attackers will call the user's mobile service provider and impersonate him,then convince the company to

redirect his text messages to a different SIM Card (**that the attackers own**) and therefore impersonating the one-time login codes.



The Telecom companies have been in cohorts(either through corruption , willingly or being strongarmed to do so) with some 'Not So Democratic' governments(for lack of a better word) to interfere with **Activists**' Social Media accounts with an intention to spy on their activities and stop them from doing their work.Recently in **Iran** and **Russia** Activists' **Telegram** Accounts were hacked when their Telegram Verify SMSs were hijacked.Short Text Messages(SMS) have a myriad of vulnerabilities on their own without being used to transmit OTPs.Fake Cell Phone towers(i.e ISMI catchers) can intercept text messages.This is done by exploiting vulnerabilities in the **SS7 Protocol**.SS7 is a communication protocol that allows telecom networks to communicate with each other.SS7 is spoofed to change a user's phone number;to intercept their SMS/Calls.Through SS7 the networks can all communicate with each other and inform them that your subscriber's using this network now,and unless your phone says otherwise,every text and call is diverted to the latter network with the attackers getting all the text messages.

This exploit is still not as easy as it sounds on paper;the attacker has to figure out the user's mobile phone number and password.Of course,this is possible with sophisticated hackers.There are better tools like SecurID and RSA proprietary user tokens and Google Authenticator App generate OTPs that change every few seconds.The code generated must match the one generated by a Web Service's server like **Gmail** and **Wordpress** ensuring that the user will enter the codes to prove their identity without the need to send them over the internet.The mechanism behind this is that when the user signs up for the service,the Google Authenticator App and Server will both start with a seed value that is later transformed into a long and unique string of characters with a hash- a mathematical expression that cannot be reversed (**Discussed in**

Detail in Chapter 4).The same string of characters is hashed again,and the results are also hashed;repeating this process every few seconds.Most of the digits of theses characters are truncated,only showing a few of them as the login codes in attempt to prevent anyone peeping and glancing at the user's phone from successfully generating their own hash chains.

Google Prompt,is a fairly new service in the market;a Two-Factor authentication that sends a Two-Factor login directly from it's servers to Android Phones or to the Google Search App for **iOS**.What would be even better is using secure systems that do not require any text messages to be sent at all.

Online Services like **Twitter**,**Telegram** and **WhatsApp** ought to look into more secure and better second-factor options other than SMSs.

Usernames and Email Addresses



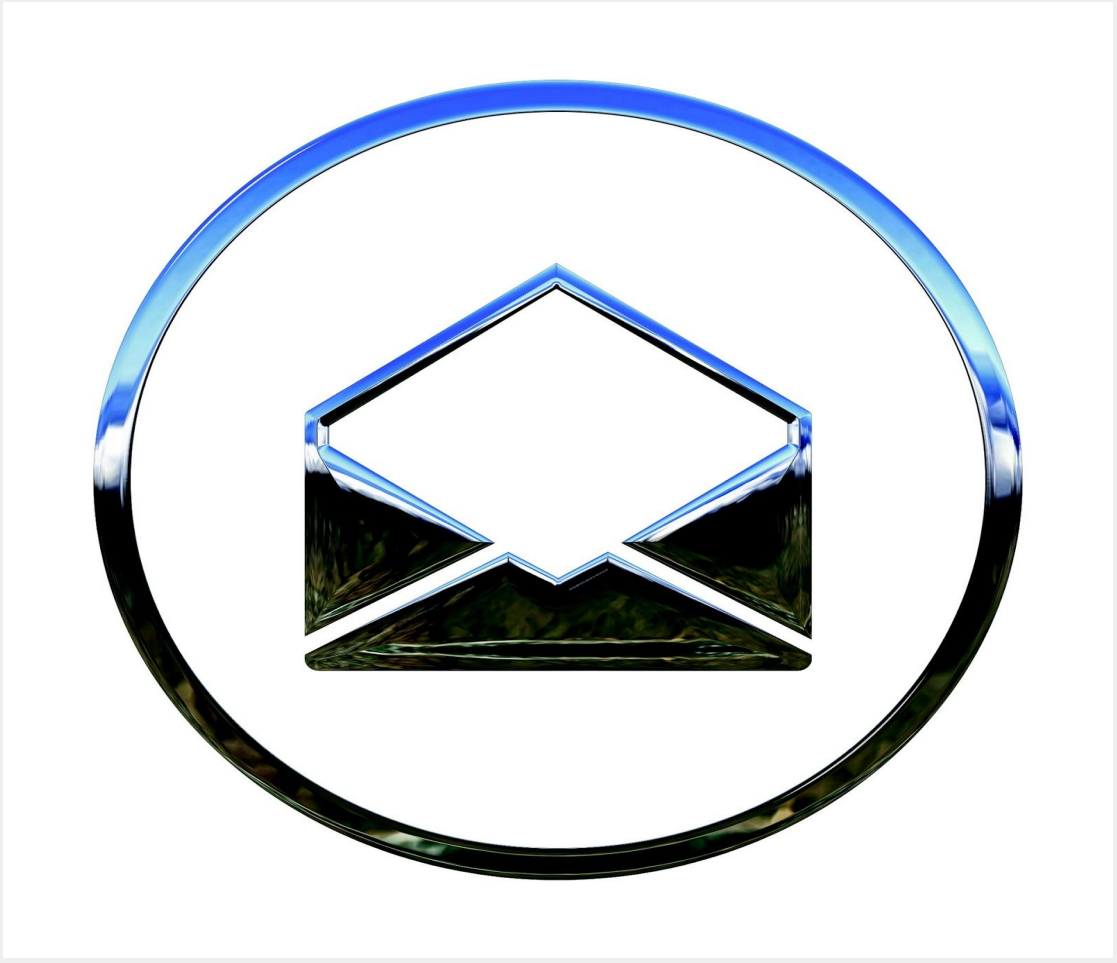
Usernames go hand in hand with passwords.When signing up to an online account,some sites will ask you to enter your email address as your username while others ask you to come up with your own username.Having a **unique username** goes a long way to secure one's accounts.It is prudent to take note of the fact that usernames are not authenticators but identifiers.A username is only there to identify which password in the database to match against.When prompted to come up with a username,most people use a variation of their real names:firsflast,first.last,firstlast80(if you were born in the year 1980.This is a very dangerous approach because your names and date of birth are on your social media profiles.We usually assume the attacker knows a great deal about you.Your email address is also available on your social media profile like Facebook.Once the attacker has your username he will try and guess the password,pretend to be you and act like he haa forgotten the password and try resetting it on some low security sites,carry out phishing or try any other method and end up obtaining your password.You should see the username as a first step to knowing your identity and **it's reasonably easier to know a**

username and try to get the password than the other way around.

	Email Address		User Name
2	Henk. Green@transsaar.nl		Henk. Green
3	Sunny. Yang@gmail.com		Sunny. Yang
4	Prascilla@innovationsmgmt.com		Prascilla
5	Berd. Tozzie@sheriff.org		Berd. Tozzie
6	Apple. Smith@sina.cn		Apple. Smith
7	Skylu2005@sohu.com		Skylu2005

In most of the Data breaches in the past Decade,a lot of details about users have being compromised:

1)**Names**
2)**Credit and Debit Card Details**
3)**Addresses**
4)**Passwords**
5)**Phone Numbers**
6)**User Names**
7)**Email Addresses**



If someone uses his/her email addresses as usernames they are in big trouble.Attackers and identity thieves could just use the username and pretending to have forgotten the Passwords,carry out password reset.They could generate phishing emails and send it to the email address masquerading as an online service and ask for sensitive information such as Passwords.It is not good to use email Addresses as Usernames at any given time.Taking into consideration all the security precautions it is also vital that the username is Simple so that you can easily remember and save you time when typing it in,you can also decide to remain anonymous when commenting on some unscrupulous or less trustworthy community sites or forums since the username appears next to each public post you make.Some online services don't provide another option,but they should stop because this puts their clients security in jeopardy.

2]Common Selection Criteria

Human Generated Passwords



The Most common way of coming up with a password is through human generation,whereby people are prompted to pick a preferred set of characters to use as the password.However,people have being noted to be notoriously poor at achieving sufficient entropy (deals with the measure of password strength in bits) to produce satisfactory passwords.People tend to come up with weak passwords most of the time.Naivety,Laziness and other factors play a significant role in people choosing weak passwords.Having stringent requirements for password strength also means that they is a high chance people will subvert the system,man doesn't like pressure and asking users to recall passwords consisting of a mix of uppercase and lowercase characters is not easy especially when you consider the limitations of the **human memory**.Creative as humans are,they are also quite predictable-patterns,repetition,humour or other techniques(Mnemonics),phrases and

words make for unforgettable passwords.Hackers know about the predictability of humans and with every data breach the results are the same; a lot of similarities and very slight differences which make password cracking something everyone can successfully do.We should therefore avoid patterned sequence or repeated characters:For Example:1111111,12345678 or qwerty,asdfgh.

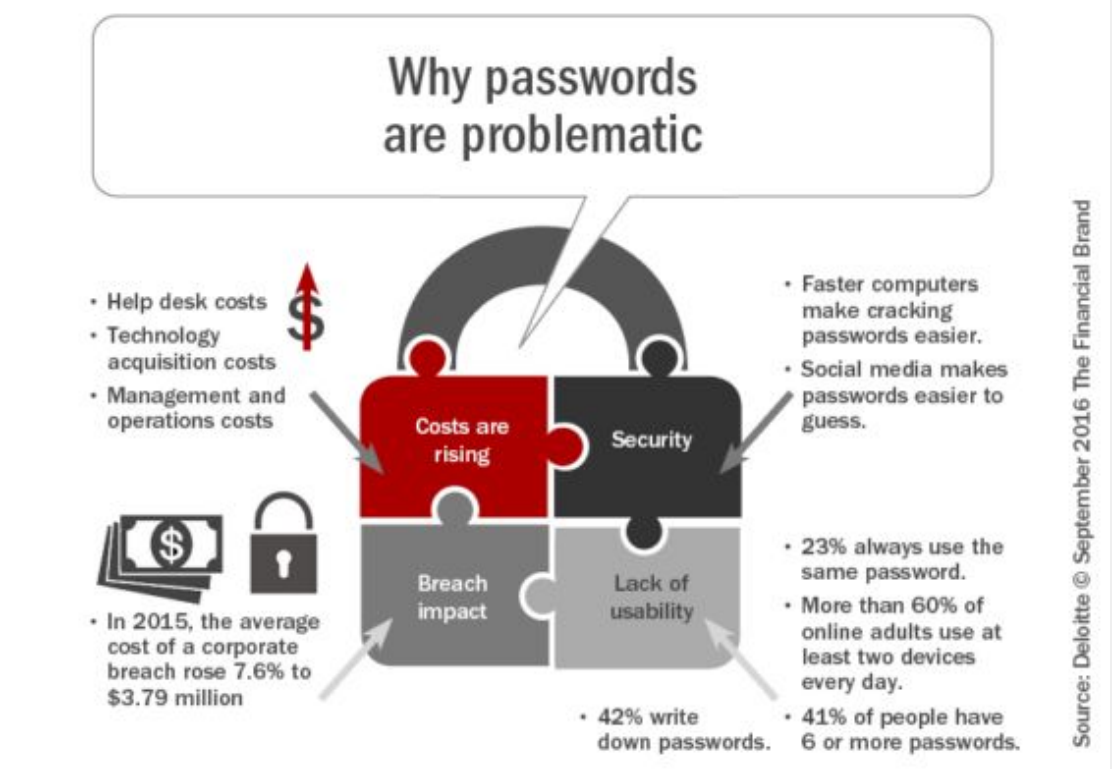
Human factors

- Can remember and repeat up to eight meaningful items
- One 8-char password
 - Can remember
- Two 8-char passwords
 - Write it down!
 - On the monitor, on the keyboard, in the wallet
- Solution:
 - *Apply a transformation t to the written down password X to generate A i.e t: X->A*
 - e.g. "Capitalize the third letter in the word and append a 2 at the end"
 - *t* is easy to remember



Weakness of Human-Generated Passwords:

I. **Choosing words short in length, that employ words found in dictionaries,easily guessable or don't properly pattern different character types.**
II. **Password Re-use whereby the same password is used on multiple sites.**
III. **Passwords others can easily find -On sticky notes found on monitors, in a notepad by the computer, whitepad reminders etc.**
IV. **Shared Passwords -users telling others passwords,sending unencrypted emails with Password information.**
V. **Default passwords which have been supplied by the system and are meant to be changed after the first login(you are even notified of this).You can research on a list of default passwords on the web.**
VI. **Using common sequences from a keyboard row like qwerty,jkl,fgh and bnm etc.**
VII. **Numeric sequences i.e 890,911,123**
VIII. **Doubled Words i.e walkwalk,lovelove**
IX. **Appending Numbers to words e.g Resource1,User1234**
X. **Using Usernames and Identifiers e.g elvis2017,4/7/1786.**
XI. **Simple Obscured words e.g j@ne and school**

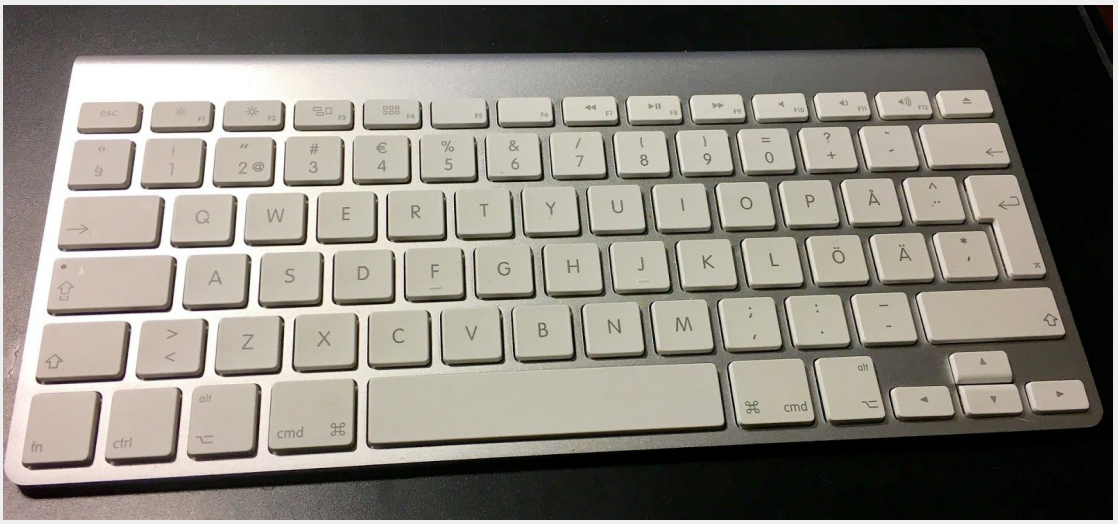


Many people are culpable of these mistakes which make it fairly easy for cyber thieves,hackers and crackers breaking into anything they can; from individual accounts,institutions,corporations of all sizes and even government agencies!

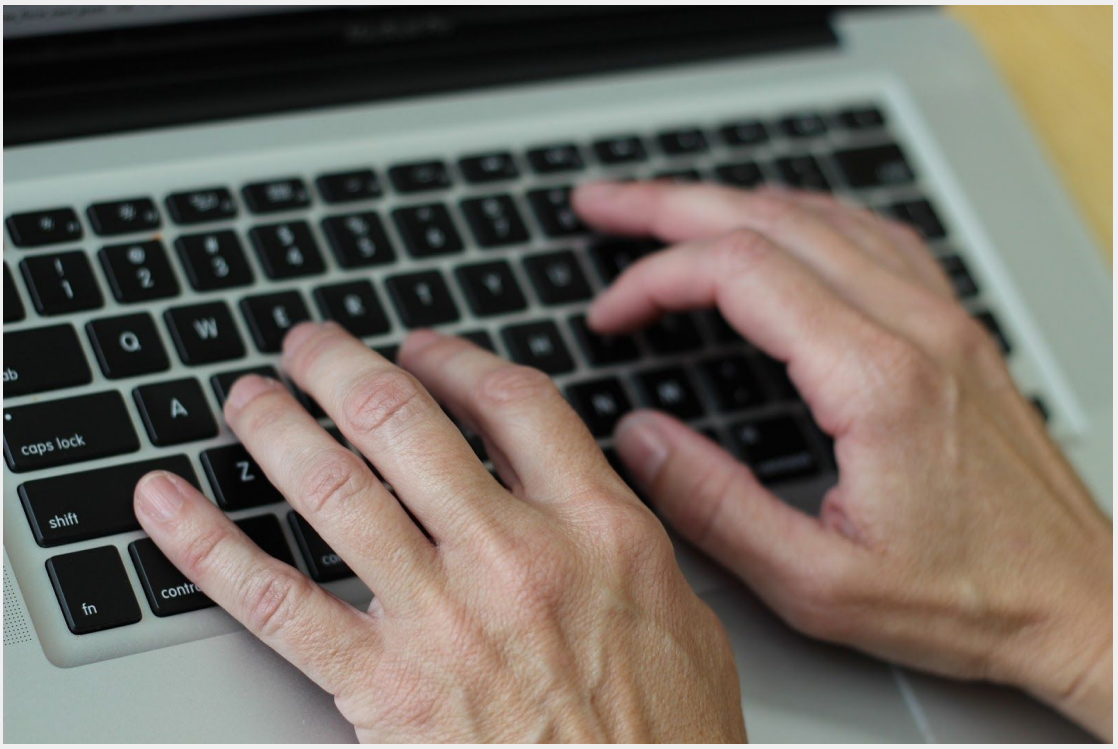
The **International World Wide Web Conference Committee** carried out a research dubbed "A large-scale study of Web Password Habits".In one analysis of over 3 million eight character passwords,the letter "e" was used over 1.5 million times,while the letter "f" was used only 250,000 times.A uniform **distribution** would have each character being used 900,000 times.The most common number used is "1",whereas the most common letters are a,e,o and r.A research conducted by **Bruce Schneier**,a Renowned Cyber Security Expert shows that users rarely make use of a large character set in forming passwords.He examined data from a 2006 phishing attack and found out that 55% of My Space Passwords would be crackable in 8 hours using a commercially available password recovery toolkit capable of testing 2,000,000 passwords per second back in 2006.Asking users to use " both letters and digits " will often lead to easy-to-guess substitutions such as 'E'-'3' and '1',substitutions which are very well known to attackers.Typing a password starting from a unique Key such as Shift key or another key is a well known trick.Password cracking has advanced at an astonishing pace.Password reuse has surged greatly and studies have shown that users average one password for 4 separate and independent accounts.Password reuse,combined with the frequent use of email addresses as usernames,means that once hackers get a hold of login credentials from one site, they often have the means to compromise dozens of other accounts, too.

Newer hardware and modern techniques have also helped to contribute to the rise in password cracking.Now used increasingly for computing,graphics processors allow password-cracking programs to work thousands of times faster than they did just a decade ago on similarly priced PCs that used traditional CPUs alone.A PC running a single **AMD Radeon HD7970 GPU**, for instance,can average about 8.2 billion password combinations each second,depending on the algorithm used to scramble them.Such speeds were only a reserve of Expensive Supercomputers and it was impossible to imagine such speeds a few years ago on Macro PCs.

Keyboard Usability Considerations



When it comes to the usability and implementation of passwords,it largely depends on the devices being used and especially hardware such as the keyboard.The 94 ASCII printable characters,presents a problem in that not all of these printable characters can be used everywhere.It is not uncommon to see recommendations to use high-ASCII characters as the ultimate secure password tip.High-ASCII characters are those that cannot normally be typed on a keyboard but are entered by holding down the ALT key and typing the character's ASCII value on the numeric keypad.For example,the sequence ALT-0255 creates the character <ÿ>.Although they are useful in some situations,you should also consider the **disadvantages**.For starters,holding down the ALT key and typing on the numeric keypad is something that can easily be noted by others.Second,creating such a character requires five keystrokes that must be memorized and later typed every time the password is entered.Perhaps a more effective technique would be to make your password five characters longer,which would actually make your password much stronger for the same number of keystrokes.Another important aspect for consideration is the National keyboard implementations which vary across the board due to other factors.Many handheld devices,such as tablet computers and smartphones,require complex shift sequences to enter special characters.Authentication programs vary in which characters they allow in passwords.Some do not recognize case differences (e.g the uppercase "E" is considered equivalent to the lowercase "e"),others even go a step further and prohibit some other symbols.Until recently did more systems permit more characters but limitations still exist.Note that all these challenges,put the user at a disadvantage such as selecting weak passwords because their powers to create and invent more secure ones has being limited.Passwords must be both reasonable for the end user as well as strong enough for the intended purpose.Forcing users to to remember passwords as we have discovered in the previous sections will only accommodate weak passwords;**a huge security threat**.



Names



A vast majority of people use names and a 123,456 or 789;appending these numbers at the beginning or end of the name e.g"name123" or "123name". Despite all assumptions and beliefs this is far from safe,and why?For starters everyone knows this as among the default passwords and it won't matter who the attacker is...some random guy in his bedroom on the other side of the world or your sly **friend** snooping around.You also have to assume that they know a great deal about you e.g Your name(**quite obvious**),family member's named,your favorite stuff and likes be it musicians,actors etc.It is also prudent to skip any real words that do exist in certain languages or from dictionaries.The **English language** has over 20,000 words.Wordlists do exist comprising over 20 Global languages.This means that it is possible to access a dictionary for any language and we could be looking at millions or billions of entries(**that are accessible to attackers**).

A 2013 Google Report on the Most Common Password types gave interesting insight;

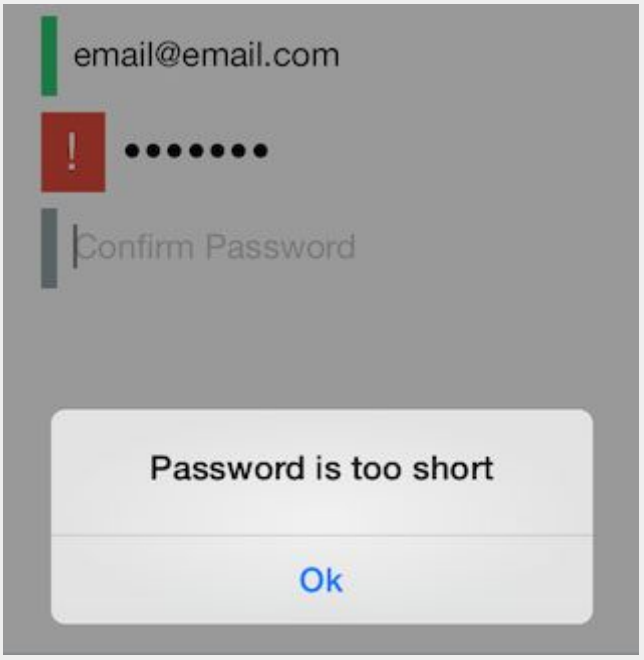
Most Common Password Types:
i)The Name of a pet,child,family members or spouse
ii)Birthdays and Anniversary Dates
iii)The word "password" (WOW!)
iv)Something related to a favorite sports team

v)The name of a favorite holiday
vi)Birthplace



As you can see,the results are the same world over;People's likings,hobbies and things related to personal info all taking centerstage and most of the time used to come up with passwords and its just not safe at all!(enough said now).The bulk of these details relating to Security Questions (**later on in this chapte**r).These are things readily available on your social media profiles and its a no brainer to get them.I highly recommend keeping away from names completely other easy to find resources could say a lot more about you than you would want or think i.e Social media could give you away easily.In almost all data breaches Names,Dates Of Birth and Physical Addresses among other details are exposed.**If your password is a name then its highly probable that you're vulnerable to an attack**.

Short Passwords



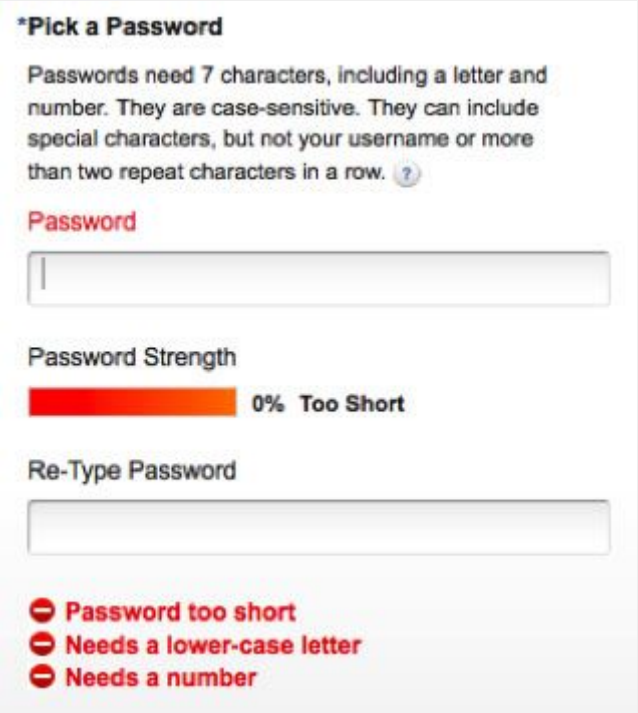
Many a times,the rhetoric has been a minimum of 8 character passwords but with our evolving world,we cannot afford to stick to one thing for too long.There is a saying that even if you're on the right track,you'll be knocked down if you just stay still.More character passwords are the way to go with the suggested minimum of 13 characters it would even be better to have a 20 character random password.It is shocking that there are sites that even today still allow people to chose 4 or even 6 character passwords(**but maybe probably because such websites do not deal with sensitive information**).Password Cracking techniques advance by the day and brute force attack,which is the main method suffers from exponential growth;the more the figure to be calculated the more time it will take to yield results and crack the password.Making passwords longer is the first step towards security.

There have been dilemma as to whether short passwords of between 4 to 6 characters with a wide variety of characters are more secure than having a long password i.e Passwords like:

1){^q™7!
2)™^9!7)
3)3-©*•C
4)©=3°%]

For starters,a good password should have a wide variety of characters so that a password cracker will have to accommodate all the characters in a keyboard e.g 103^4 or 103^4...which is not mathematically a bigger number than 103^8or 103^13.In case the password only contains lowercase and uppercase characters;52^8 is still a bigger number than 103^4 or 103^6.The short passwords with a wide variety of characters will be cracked faster than longer passwords with a minimal variety of characters or longer passwords with a wide variety of characters.Use longer passwords all day,any day and if you use

a wide variety of characters the better.



Any Significance Of Using Spaces in a Password?

What to do	Example
Start with a sentence or two.	Complex passwords are safer.
Remove the spaces between the words in the sentence.	Complexpasswordsaresafer.
Turn words into shorthand or intentionally misspell a word.	ComplekspasswordsRsafer.
Add length with numbers. Put numbers that are meaningful to you after the sentence.	ComplekspasswordsRsafer2011.

There is the usability issue- in that spaces are hard to visually make sure you typed correctly if the password is not hidden.The space bar also makes a unique sound when tapped,someone will easily hear you do it.Spaces are not in any category of character sets;they are neither letters,symbols nor numbers.Spaces do not make the password complex or stronger even by a small bit.The space character ' ' or " " is quite different from 'a' or 'bb'.The blank space character may also be seen as other characters,such as new lines

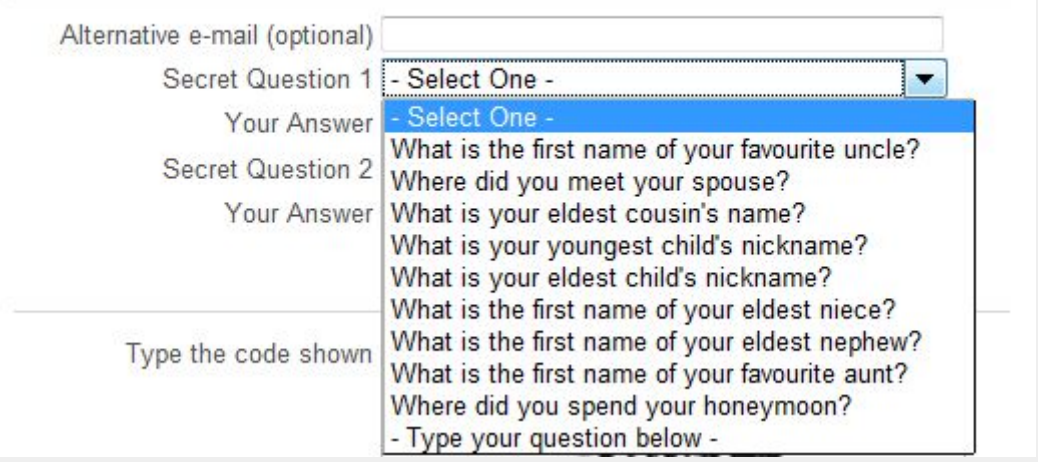
-'\n'.Programs handle blank spaces differently,spaces in filenames maybe parsed by adding a % to it to do away with the space e.g My Space will equate to My%Space while other programs trim blank characters(such as newlines,tabs and spaces) if they happen to come at the beginning or end of a field.This trimming largely aims at discouraging people from copying and pasting incorrect data.

Not having spaces in passwords avoids a lot of problems and saves support calls(because the user tries to type in a password with a space,but the space was trimmed and the user cannot understand why the password is wrong!)this in case there was no dialogue when the space was trimmed.It has even being described as a useless feature that does nothing at all to contribute to password complexity or strength.Using spaces might even encourage users to use sentences as passwords.

Security Questions

If you have ever forgotten your password and you want to reset,you may have been prompted to answer some questions;such questions are known as security questions.Security Questions are meant to provide an additional layer of security especially to online account logins;they are mostly handy when a user forgets a password and wants to reset it.Security questions can be classified as Good,Fair or Poor depending on various issues thus a **good security question should produce answers that are;**

1)**Safe(not guessed)**
2)**Stable- Do not change overtime**
3)**Memorable**
4)**Simple**
5)**Have many possible answers**



They however come with the following challenges:

1. **Some users use the answers to these questions as their passwords(discussed previously in names)**
2. **With the advent of social media the answers to most of these**

questions are easy to answer because of the info in your social media profiles, therefore an attacker will pretend to be you and continue to the option of Forgot Password.Here he will just answer the security questions submitted to him and voila he's got his 'dirty' hands on your data,financials and whatever else you have in there.

Gartner Research recently found out that the so called self-service challenge questions can save companies between $51-$147 for each password reset question handled through the web rather than by a phone call!From a business perspective the idea is always to minimize cost but at what cost to the clients? Think of the thousands of identity theft cases because it is easier to impersonate someone over the web than over a phone call.Customers who don't protect themselves are highly prone to such crimes.This scenario reminds of a saying about online services and their we their users -"**If you do not pay for the service then you're not the client but the product**".It simply means that if you are not charged anything then you're the product;in terms of the data they have about you.These services do not care a lot or at all about your security but I think its high time they do.They should be willing to spend money on us because without us then definitely,there is no them,right?Not all of them however,are inclined to that mode of operation but there is still a long way to go and we could all do with better service.We could avoid these challenges by making a habit of **Reading** the Privacy Policy Section before happily signing up for every website.We either say Accept and Continue without reading or don't even look at the section at all(Please take it upon yourself to always Carefully go through the Privacy Policy).Anyway,I hope the point home is home and more on that some other time.

Most of the Security Questions are usually:

I. **What is your favorite book?**
II. **What is your mother's maiden name?**
III. **What was the name of your first/current/favorite pet?**
IV. **What is your favorite food?**
V. **What is your favorite place to vacation?**
VI. **Where did you go to high school/college?**
VII. **What City were you born in?**
VIII. **What was the first company that you worked for?**
IX. **What is the name of the road you grew up on?**

Researchers at Microsoft and Carnegie Mellon came up with a report that documented how people with absolutely no prior knowledge of the person whose account they were hacking...were able to guess the correct answers(told you so) 15% of the time.Why?because as we have severally stated the majority of these questions are topics that are common material for social network profiles and updates.Well,one would probably result to limiting the privacy setting of your social network updates to friends only,that's all there is to it?I'm definitely safe as one can be now.This is not entirely true because did you also limit your profile information?Probably not.

Identity thieves can use stolen information for more than just financial fraud.A correct guess to just one security question can give the thieves all the information to do the following:

I. **Look up the answer to "what is the name of the road you grew up on?" Using a public records search or finding it on a forum or social network.**
II. **Find the answer to "where did you go to high school/college on your LinkedIn.**
III. **Guess the answer to" what is your favorite food?"by viewing your Twitter feed and more.**

With this they can even pose as you and unlock your account on any website-from social networks to online banking portals,get clearance during a traffic stop or get services at a hospital!In all certainty the identity thief can do a lot of harm(we all have of the many endless cases of identity theft)and therefore login security questions should not be taken lightly.It is important for online services to encrypt Security Questions and answers.In December 2014,**Yahoo** was dealing with the biggest data breach in History(between 2013-2014)- Over 1.5 Billion Used Accounts had been compromised.These hacks were carried out in 2 phases.In the **Second Phase**,which was carried out by a different group of hackers from the first one,1 Billion Accounts compromised;with Names,Date Of Birth,Email Addresses and Passwords but most unbelievably Security Questions(**Unencrypted or Not**) were compromised!

Random Things

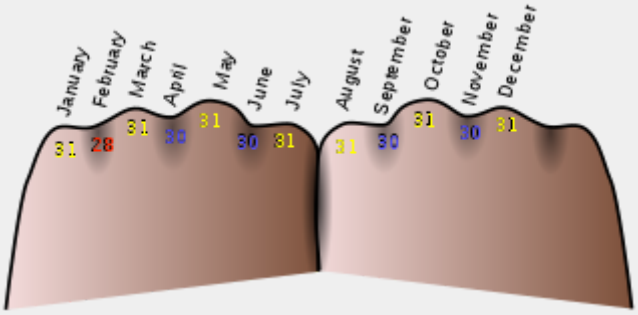


What if I try throw in random stuff,say maybe a phrase or word I like e.g a word in the urban dictionary or some popular phrase in the **public domain?**I guess I should be safe?In the case that the word is not a real word then it is likely you're secure.Real words are susceptible to dictionary attacks.The average attacker will try different techniques to crack the password,as we have already discovered.They will start with Names and a 123/789 before or after the word and if they don't succeed random things is the next thing and they do this via the Dictionary Attack method.It turns out that,a really strong technique is passphrases.This technique involves opening several pages of books or magazines and putting your finger on the text.Write down these words and mash them up to form a passphrase.However such techniques have become quite popular in recent times,attributed to copycatting.If people find something that works then all of them try to do the same without adding a bit of creativity or variation,and the attackers know this too.



Example:let's use selfie(and don't ladies love them)as our sample password.
(i)123Selfie/Selfie123 or 789Selfie/Selfie789
The password is weak despite using an uncommon word.It's true that the word Selfie has been in the urban dictionary for a bit of time now;the word Selfie was incorporated as an official english term through the 9th Edition of the Oxford Dictionary.All the other dictionaries have most probably followed suit by now,so in a dictionary attack you'll be caught flat footed.The numbers 123 have also being appended in a very predictable way(as always);at the beginning or at the end– that is where the attacker starts,until he figures out that you've appended numbers/symbols or not.If not he will move on to other techniques.

Mnemonics



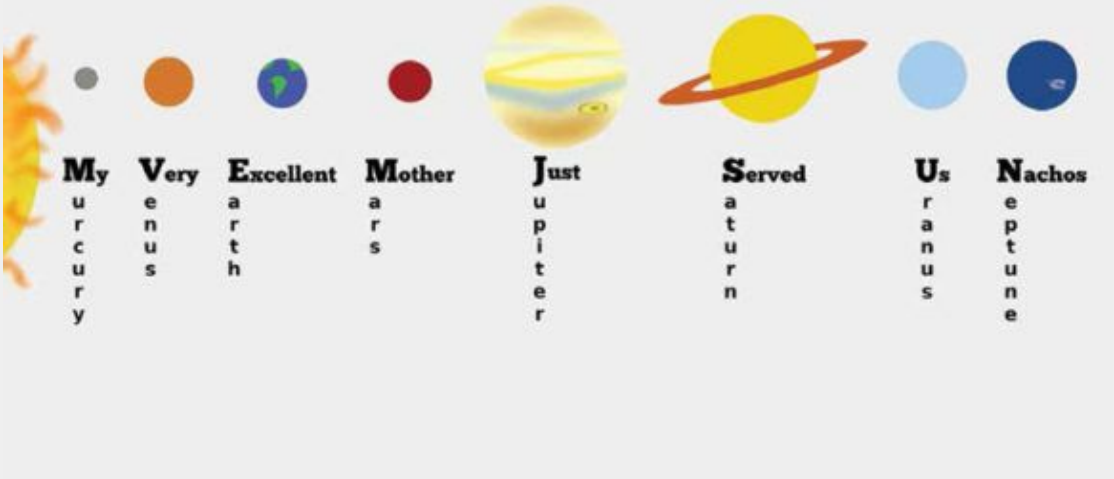
Mnemonics(pronounced as nemoics,the M is silent) are learning techniques that aids information retention in the human memory.I guess everybody knows 'ASAP'.The application of mnemonics is based upon the observation by scientists that the human mind more easily remembers personal,physical,sexual,surprising and any other information that it can easily relate to,in contrast to more abstract forms of information.They employ elaborative encoding,imaging and retrieval cues as specific tools to encode

information,and associates it with something more meaningful thus allowing the brain to have better retention of the information.Mnemonics are also oftenly used for lists,in auditory form such as poems,acronyms or memorable phrases.Mnemonics are in many categories:

(1)Name Mnemonics
(2)Music Mnemonics
(3)Expression Mnemonics
(4)Ode Mnemonics
(5)Model Mnemonics among others.

Their main advantage is that they use information stored in long-term memory to make memorization an easier task.

There are many common examples of Mnemonics,used in day to day to life *e.g the knuckle mnemonic used to determine months with 30 or 31 days,the Roy G. Biv for colors of the rainbow(Red,Orange,Yellow,Green,Blue,Indigo,Violet).*



*Another one I vividly remember from my early school days is the one used to memorize the names and order of the 9 planets of the universe-My Very Educated Mother Just Showed Us Nine Planets(that is Mercury,Venus, Earth,Mars,Jupiter,Saturn,Uranus, Neptune, Pluto).*As the above examples prove,it's quite easy and people might employ Mnemonics to make the passwords easier to remember but it may also be used when passwords have to be repeatedly changed;this is the main reason behind mnemonics.Whether or not the mnemonic is your creation or is in the public domain doesn't matter;a dictionary attack will retrieve these passwords because of the fact that they are mostly purely characters(one or two digits following each other) and they follow patterns.

Example:(i)Take the initials of each and every month of the year backwards.
>DNOSAJJMAMFJ/dnOsajjmamfj/Dnosajjmamfj/dnosajjMamfj x
ii)Take the initials of the subjects you took at school.In any order e.g say you did French,Maths,Chemistry,Biology,Business,English,History,Italian and Geography.
>FMCBBEHIG/fmcbbehig/FmcbbheiG/fmcbBheig x

Numbers and Symbols



The *@#$%&!?*'¶√£¢€¥^°=©®%™[]\<>,.}{×÷π•`|~/;:*-0123466789* of this world!

Adding symbols and numbers to a password?The positioning of these symbols and numbers on the keyboard and more so on the password does indeed

matter a lot,otherwise you'll be going through a lot of trouble for nothing.Consider a scenario in which you have used symbols or numbers that follow each other in a certain order or say after a certain keyboard key or counting several rows?It is more likely that the trick is also known by other people out there.Users will also more often than not come up with easy-to-guess substitutions like 'E' for '3' and 'I' for '1'.You should be careful because most of these numbers have something to do with the months or year of birth in most cases.The password is vulnerable to password mangling rules for use with password cracker tools and the brute force attack.If a certain model doesn't work say they have tested both uppercase and lowercase characters and still the password hasn't been cracked,it will replace the characters with numbers and symbols.

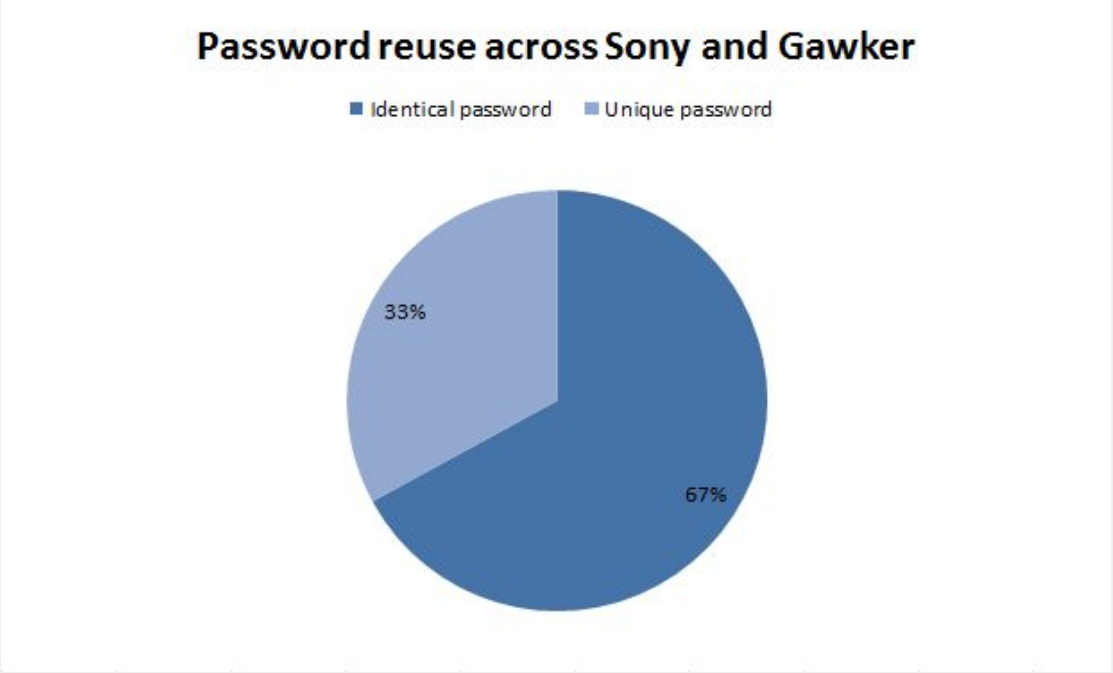


Example:let's still use Phoenix as our sample password.
(i)Phoenix17%& x
(ii)@™Phoenix17. x
(iii)Phoe&17nix x
Note that in both examples (i) and (ii),the symbols and numbers are appended at the beginning or end of the word.In example (iii) we have put the symbols and numbers in the middle but when password

mangling is applied the password will eventually be cracked.However this password may take last longer than those in (i) or (ii) as it needs another technique to be used.

Reusing Passwords

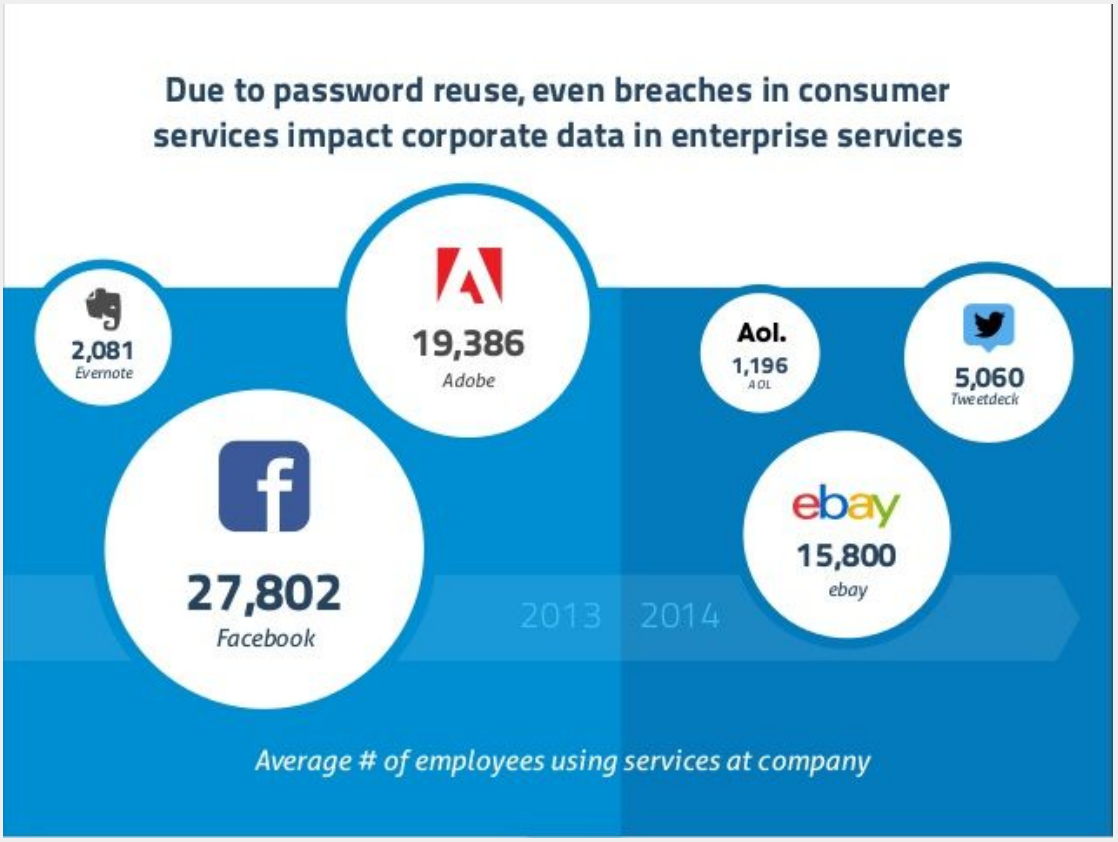




Admit it,we are all guilty of committing this 'crime'.We talked about the limitations of the human mind and how we detest pressure and stress situations very much,it therefore becomes very tasking to have a password for each account.We can't afford to remember all those passwords so we just lazily use the same password everywhere.Sadly,this only makes the attacker's work easier.In every data breach many user details are leaked and among them usernames and passwords.The attacker will try such usernames and passwords on other accounts he can think of such as Gmail,Twitter etc and if the password is the same then you're done for!I have seen some people give wrong advice...That **you use variations of the same password;only appending different numbers and or symbols to it.This is plain**

wrong because first we should not reuse passwords and we've also seen that appending numbers/symbols is not a very good idea.

Example:(i)let's use Phoenix as our sample password.
So for Twitter,Facebook,Gmail and Instagram Accounts password is Phoenix17$&/@™Phoenix17.The password in itself is weak and poorly selected but still someone goes ahead to use it in all his accounts.As we said,if one account is compromised it will be quite easy to do the same on the other accounts.



Sharing Of Passwords



Sharing of passwords is a very common vice in the realm of Cyber Security,it might not have any major repercussions if you share your passwords for your personal data with say a spouse or friends.However,in corporations or organizations,the scenario is quite different because people are given access to resources according to their job rank and designation,and sometimes given the prestigious title of the Administrator or Admin(**Tag a WhatsApp group Admin**).They are the only ones who have access to the resource or information in the organization or company.This is quite in order,but it becomes an issue when the admins share the password with people who are not authorized.Some of these scenarios could lead to serious integrity issues at the firm with data,finances and reputation of the Organization being at risk of being compromised.Separate logins are better because they can be used for accountability checks e.g-to know who changed a certain piece of data.Therefore users should have individual passwords despite having the same role and should also be held accountable for their actions(especially dealing with their account management).



Mangling/Mirroring/Turning It Around

This is where people tend to think that enna is much more safer that anne.The creativity behind this is good,and it should only be used to come up with a nickname.Thinking that enna is safer than anne is purely wishful thinking according to me.Turning around a password does not increase the keyspace(**length**) of the password and directly so even password strength.Mirroring the password from how you had initially created it,doesn't make the password any stronger in any way.

Usernames and Email Addresses

As we discussed in chapter 1,it is not wise to use Email Addresses as Usernames because**:(1)**The email address is everywhere in your social media profiles**(2)**Real Names and other user data is compromised every time a data breach occurs.There are various ways to go around this challenge:

(I)Create a username that is different from your e-mail address:Usernames are accessible to anyone and you should create unique Usernames that do not in any way relate to your Real Name or your nickname (which is on your Facebook profile)

(II)Skip Personal Details

No ages and Year of Birth,Addresses etc because this data is readily available in case of a data breach and you'll be in trouble.Use both numbers and symbols to create your email address,this will also save your address from spammers who use dictionary attacks to email thousands of possible name combinations(after obtaining real names from data breaches) at large **Internet Service Providers** or email services (e.g **Hotmail**,**Yahoo** and **Gmail**),hoping to find valid addresses.

(III)Multiple Addresses

Have more than one email address and use one to "**sacrifice**" to register to those sites that only or mostly use Email Addresses as the Usernames,register to less familiar websites,forums and blogs or to create accounts for making purchases online.

3]Password Cracking

Cracking Passwords



Password cracking refers to various means used to discover computer passwords.This is usually accomplished by recovering passwords from data stored in,or transported from,a computer system.Password cracking is done by either repeatedly guessing the password,usually through a computer algorithm in which the computer tries numerous combinations until the password is successfully discovered.Password cracking can be done for several reasons,but the most **malicious reason** is in order to gain unauthorized access to a computer without the computer owner's awareness.This results in

cybercrime such as stealing passwords for the purpose of accessing banking information.Other,non malicious reasons for password cracking occur when someone has misplaced or forgotten a password.Another example of non malicious password cracking may take place if a system administrator is conducting tests on password strength as a form of security so that hackers cannot easily access protected systems.Password-cracking computers working in conjunction with each other are usually the most effective form of password cracking,but this is time consuming.There are two types of website's compromise from which user's passwords can be recovered,this attacks are in the Bruteforce category:

(I)Targeted Attacks - In this case a hacker targets a single user and tries to access their account.The basic formula for this is to pick a target,guess the username,then guess the password.Email addresses are the most common usernames for most websites,are fairly easy to get a hold of(**from social media profiles**).Other times,however user's pick a username separate from an email address,but most people still use some variation on their real names: firstlast,first.last,firstlast87(**year of birth**).If the attacker doesn't have a particular target then decoding an encrypted database is the next option.They gain access to a lot of individual's data,and this breach can affect hundreds to millions of people at once.Most of the techniques used for targeted attacks are;Brute Force Attack,Dictionary Attack and Key Logging.

(II)Database Compromise - Exploits such as SQL and XSS Injections of malware into databases to gain access or other methods.The main idea is to decode encrypted databases where passwords are stored and try to gain people's data to be used in hacking escapades and exploits.



Dictionary Attack



For example a password like bosn97Newas is made up of 'bosn9' + '7Ne' + 'was' and is not a safe word combination.The word is composed of three components: **1)** The string 'bosn9' follows the pattern [dictionary word][**one or two digits**].**2)** The string '7Ne' follows the pattern [**one or two digits**][dictionary word].3) 'was' is actually an actual word thus a dictionary word.

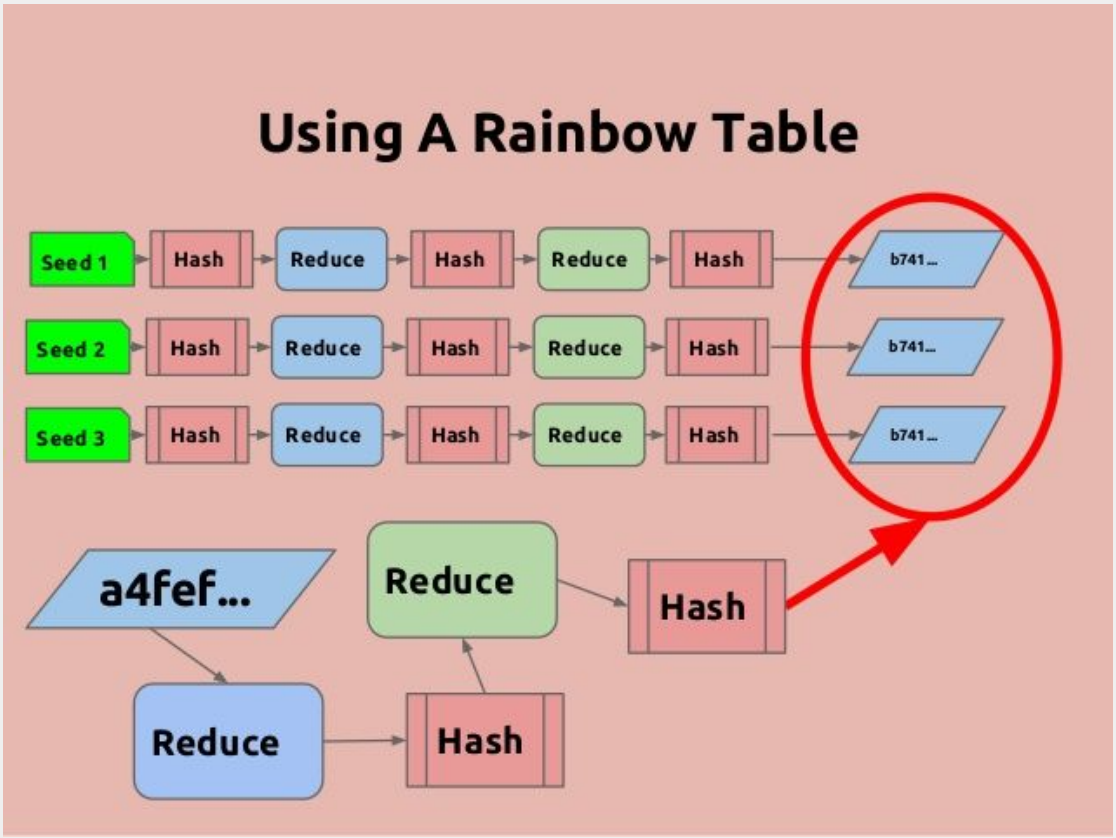
A dictionary attack is the easiest but not simplest route to start cracking passwords but not quite fastest password cracking attack.To put it simply,it just runs through a dictionary of words trying each one of them to see if they work.The criteria for a password to be cracked through the dictionary method is;The password is broken down into at least 3 components of about 3 or 4 characters.In component,there are one or two digits that follow each other and real words from dictionaries,for example looking at the The string Bosn97Newas>'Bosn9' follows the pattern[dictionary word] [one or two digits],'7Ne' follows the pattern [dictionary word] [one or two digits] and 'was' is a dictionary word.Computers very fast run through millions of words in a few hours.This should usually be your first approach to attacking any password,and in some cases,it can prove successful in mere minutes.It tries patterns such as "aaa", " aab", "aac" and so on.**Wordlists** are used to carry out dictionary attacks.

Dictionary words have a high degree of pattern similarity (think how many words have “ion” “tion” “ea” “qu” and so on),and if you compare a large data set (**like a big ol’ pile of passwords**) to a list of common patterns in the English language, you’ll see that it’s really hard to make them look different

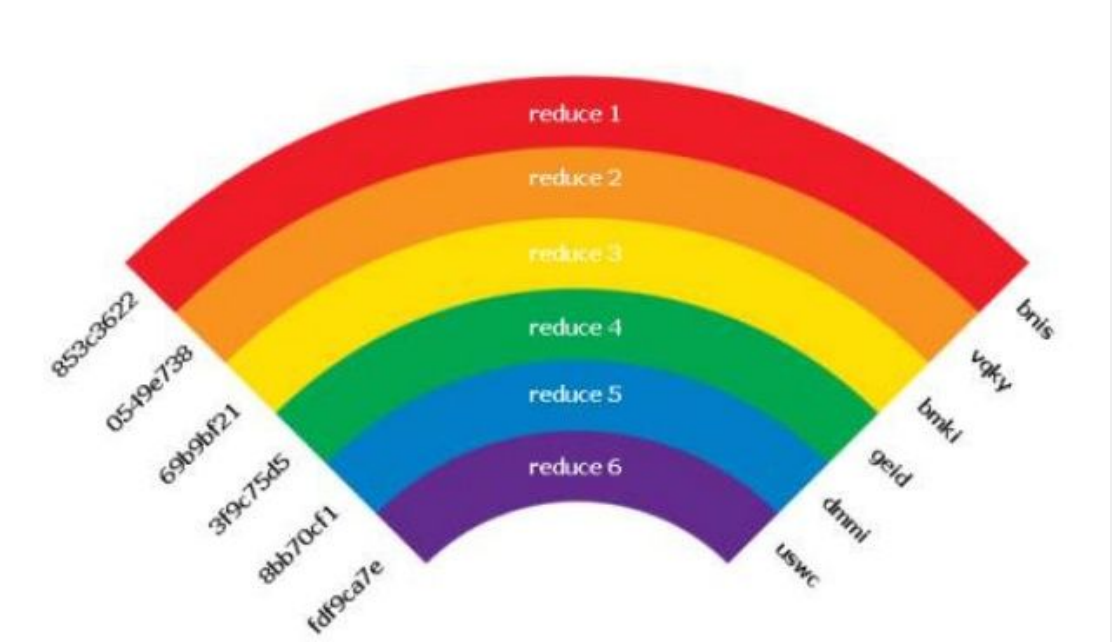
enough to be both random looking to a computer and memorable to a human. After the **RockYou** breach,everything changed.Password crackers abandoned wordlists compiled from Webster's and other dictionaries which had been modified to try and mimic the **words**(as passwords) people had been using to access online services.In their place,they adopted a collection of letters,numbers and symbols plus cartoon characters and pet names which was something unheard and unthought of before;this would now be the basis of future attacks.



Rainbow Table



Most modern systems now store passwords in a hash.This means that even if you can get to the area or file that stores the password,what you get is an encrypted password.One approach to cracking this encryption is to take a dictionary file and hash each word and compare it to the hashed password.This is very time and CPU-intensive.A faster approach is to take a table with all the words in the dictionary already hashed and compare the hash from the password file to your list of hashes.If there is a match,you now know the password.Here you create precomputed tables for reversing cryptographic hash functions.The tables are usually used in recovering a plaintext password upto a certain length consisting of a limited set of characters.



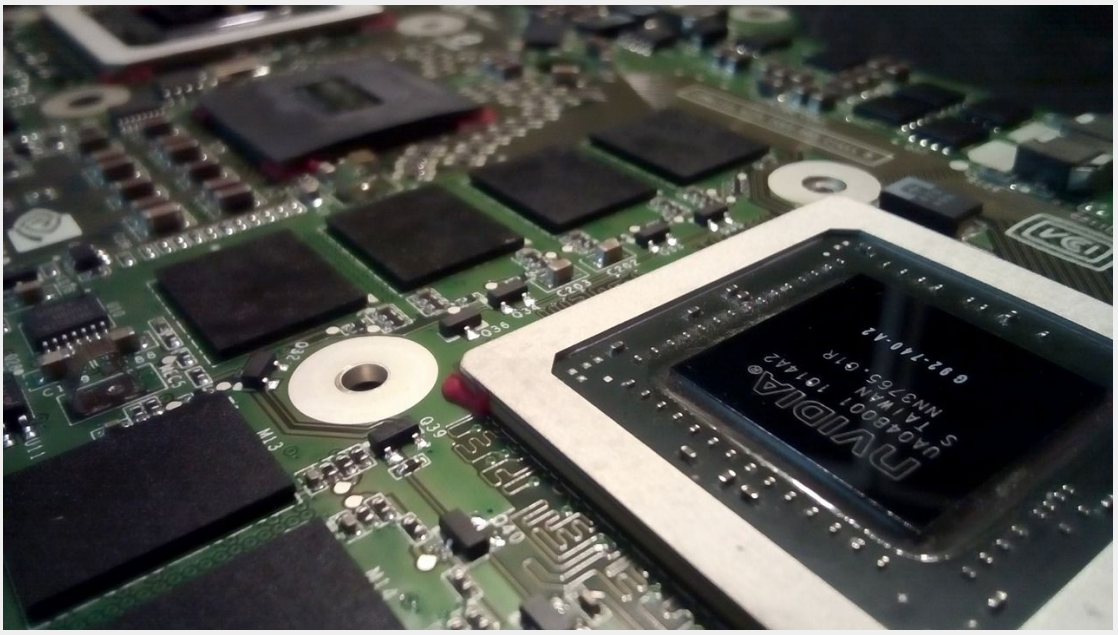
Brute Force



Brute force is the most time consuming approach to password cracking. It is always the attackers last resort.Brute force password cracking attempts all possibilities of all the letters,number,special characters that might be combined for a password and attempts them.As you might expect,the more computing **power** you have,the more successful you will be with this approach.Password wordlists exist in almost every language and are used with

password cracking tools to carry out bruteforce attacks.

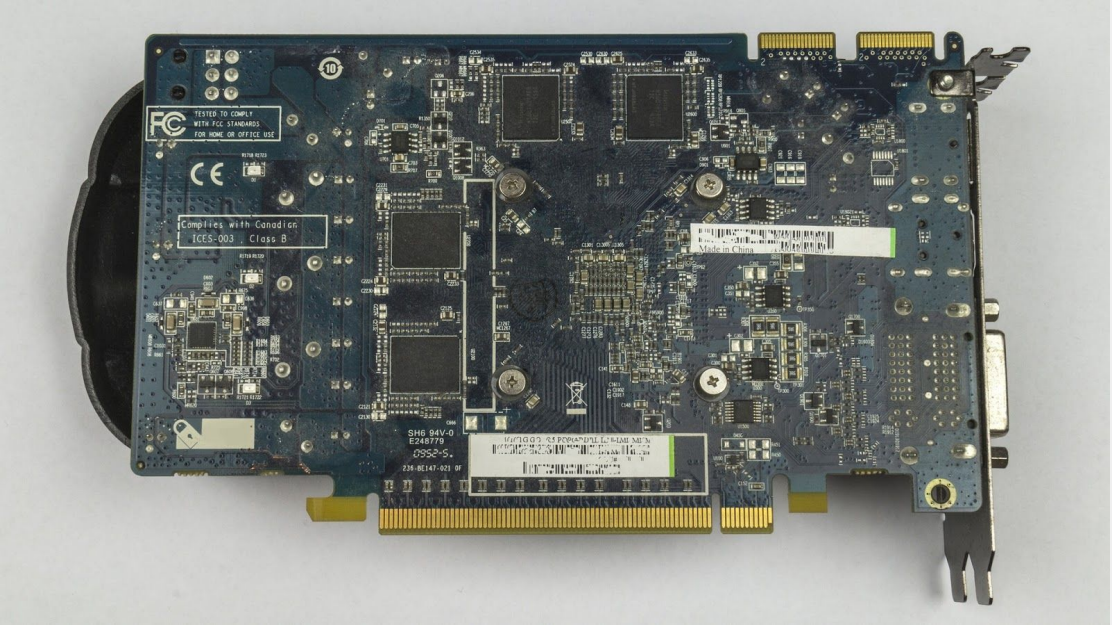
GPU



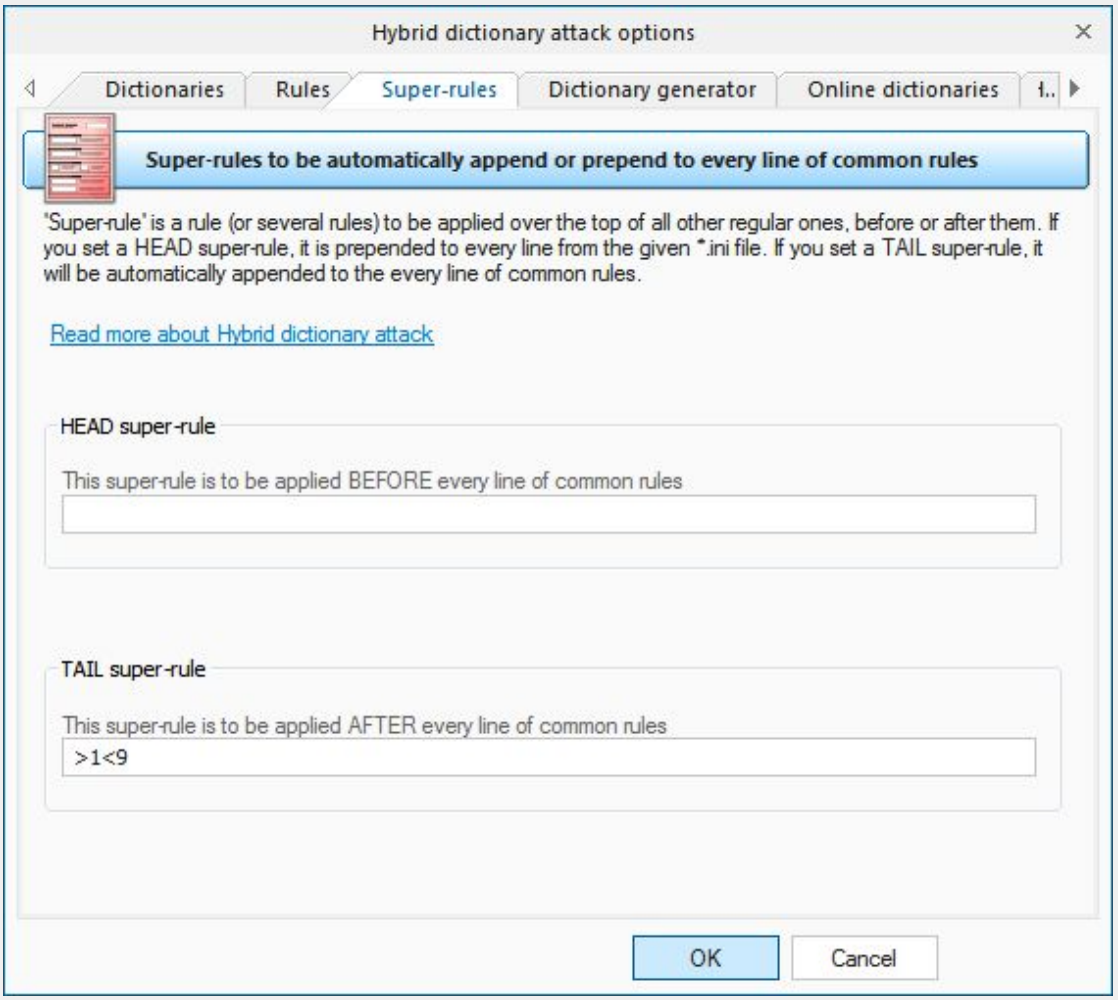
GPUs,or graphical processing units,is a processor whose task is calculating the graphical output for monitors.Mostly used in computers and video game systems.They are much more powerful and faster than CPU for rendering graphics on your computer and for cracking passwords.GPU's calculations go beyond simple calculation and output of pictures.Calculation of Physics,Artificial Intelligence (AI) or even acceleration of video and picture editing make GPUs a very effective tool in hacking- cracking of passwords due in part to its speed of execution.Another implementation of GPUs is 2D and 3D Acceleration.The main manufacturers of GPUs are **Intel,nVidia** and **AMD**(operate under the label of **ATi**).

For example,as we have already discussed many website users have a tendency to append years to proper names, words, or other strings of text that contain a single capital letter at the beginning. Using brute-force techniques to crack the password Elvis1990 would require 629 possible combinations, a "keyspace" that's calculated by the number of possible letters (52) plus the number of numbers (10) and raising the sum to the power of nine (which in this example is the maximum number of password characters a cracker is targeting).Using an AMD Radeon HD7970, it would still take about 19 days to cycle through all the possibilities.However,Using features built into password-cracking apps such as Hashcat and Extreme GPU Bruteforcer, the same password can be recovered in about 90 seconds by performing what's known as a mask attack. It works by intelligently reducing the keyspace to only those guesses likely to match a given pattern.Rather than trying aaaaa0000,ZZZZZ9999,and every possible combination in between,it tries a lower- or upper-case letter only for the first character,and tries only lower-case characters for the next four characters.It then appends all possible

four-digit numbers to the end.The result is a drastically reduced key space of about 237.6 billion, or 52 * 26 * 26 * 26 * 26 * 10 * 10 * 10 * 10.



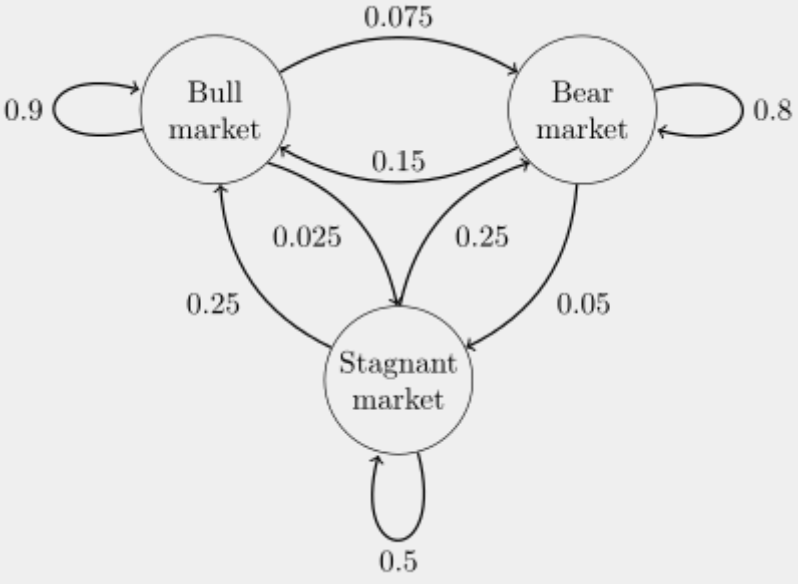
Hybrid Attack



A hybrid password attack is one that uses a combination of dictionary words with special characters,numbers,etc.It can even marry a brute force attack;with such a combination greatly expanding the reach of a well grasped wordlist while keeping the keyspace to manageable lengths.Often times these hybrid attacks use a combination of dictionary words with numbers appending and prepending them, and replacing letters with numbers and special characters.For instance a dictionary attack would look for the word "password",but a hybrid attack might look for "p@$$w0rd123".Other examples are LOL1313le" , "Coneyisland9/," "momof3g8kids," "1368555av," "n3xtb1gth1ng," "qeadzcwrsfxv1331," "m27bufford," "J21.redskin," "Garrett1993*," and "Oscar+emmy2."A hybrid attack follows a set of rules to greatly expand the number of passwords wordlists can crack.Rather than brute-forcing the five letters in Elvis1990,hackers simply compile a list of first names for every single Facebook user and add them to a medium-sized dictionary of say,100 million words.



Markov Chains - This is a mathematical system,which statistically generates brute-force attacks.Hashcat(password cracking tool)makes it simple to implement this method.



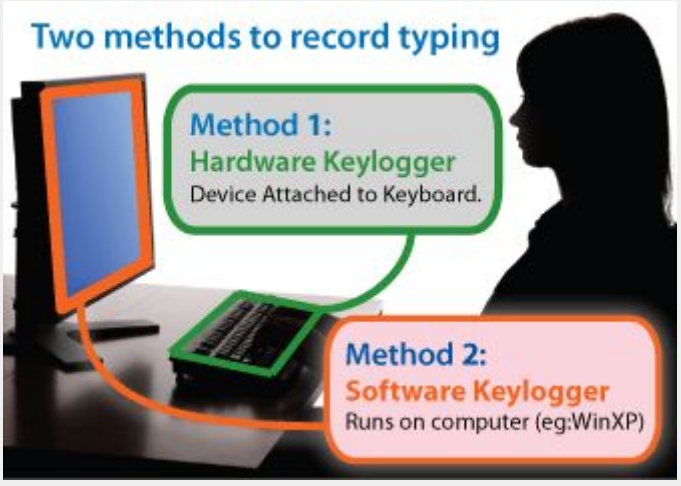
By looking at the list of passwords already cracked,it performs probabistically ordered, per-position brute-force attacks.A classic brute-force attack will try " aaa","aab","aac" and so on but a Markov attack makes highly educated guesses.It analyzes plaintext passwords to determine where certain types of characters are likely to appear in a password.A Markov attack with a length of seven-character passwords,with the 65 most likely characters for each position and drops the keyspace of a brute-force from 95^7 to 65^7;in effect saving the attacker four hours.Passwords show starking degrees of uniformity when it comes to the types of characters in each position - Uppercase letters at the

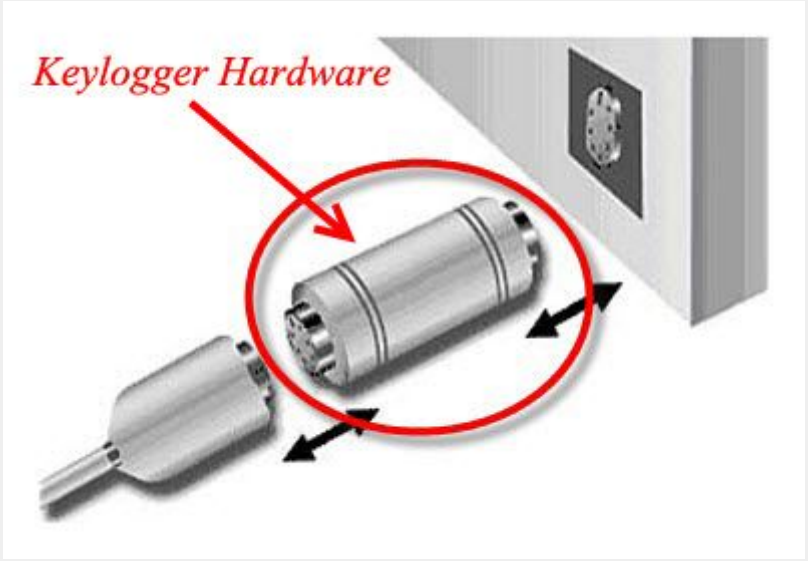
beginning,Lowercase letters in the middle and symbols and numbers at the end thus making Markov attacks almost more effective than straight brute-force attacks.

Combinatorial Attacks

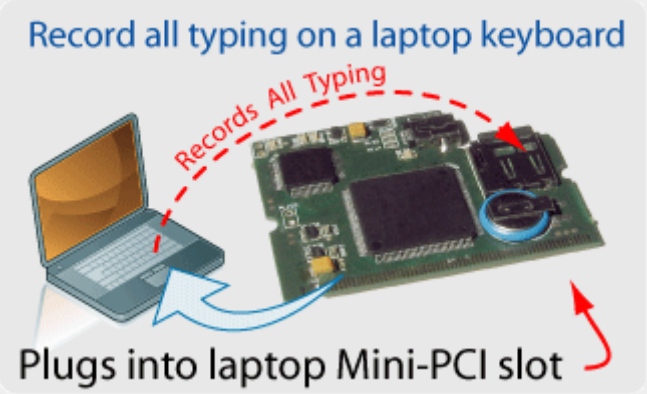
This kind of attack combines each word in a dictionary with every other word in the dictionary.Hackers and Penetration testers have hailed it as the answer to the **"batteryhorsestaple"** or **"medicineshoegrass"** thing where people just pick up a bunch of words,mash them up and then claim to have a **secure** password.

Keylogging



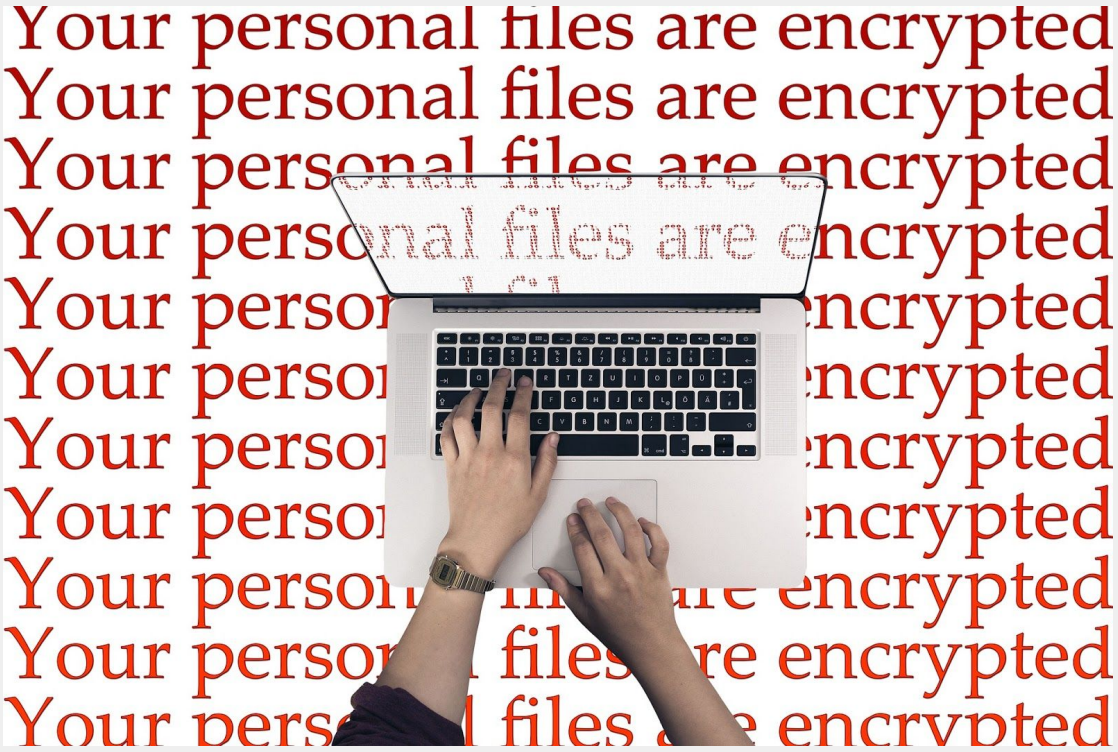


This is a method which relies on getting a piece of malware onto your computer that watches what you're doing and keeps track of what you're type,sending that information to a hacker.It in fact records your password as you type and the attacker doesn't have to guess anything.Keyloggers are malware,and therefore good browsing behavior is Paramount,to avoid picking up harmful things (**a good rule of thumb is to always never download and or run files from an untrusted source**)



Protecting against keylogging is both simpler and more complex than the other forms of attacks.Copying and Pasting passwords from a password manager,or using an auto-fill ensures that you're never really type the password at all,so you don't have to worry about the keystrokes being logged(Although there are some limitations and downsides to doing this).

Encryption and Cryptography

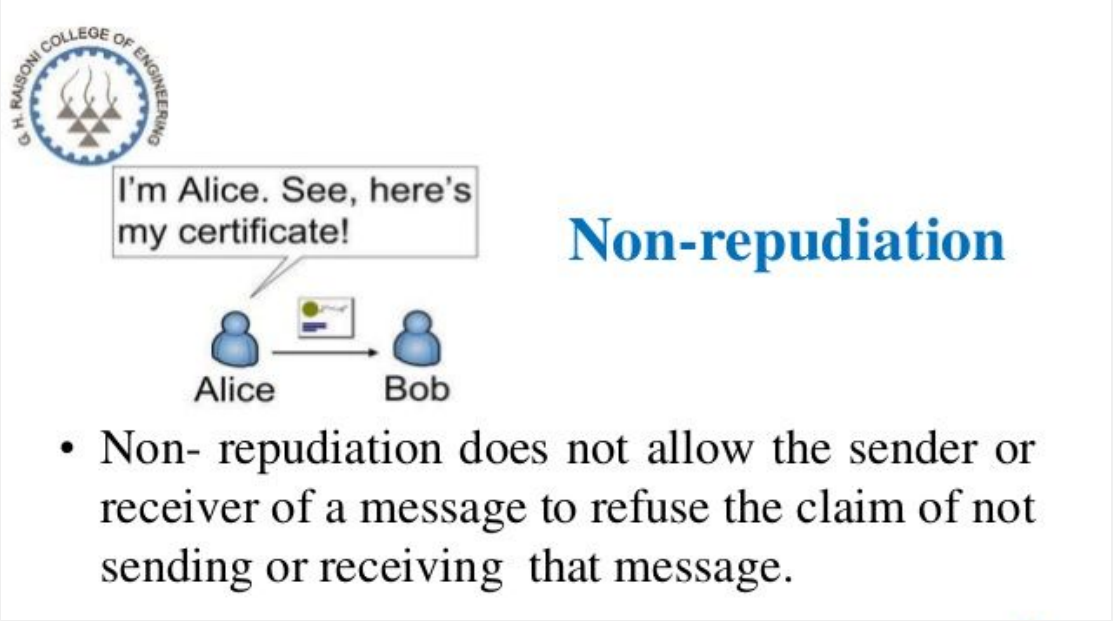


Encryption is the conversion of electronic data into another form,called ciphertext,which cannot be easily understood by anyone except authorized parties.The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet such as Emails or other computer networks.The data is scrambled to make it unreadable to unintended parties.To decrypt the message one has to have the passcode.



Cryptography on the other hand,is the science if encryption and Cryptanalysts are scientists who deal with Cryptography.
There are two main types of encryption: Symmetric and Asymmetric.The most common and popular encryption algorithms are **Triple DES**,**RSA**,**Blowfish**,**TwoFish** and **AES**.The Size and Key of an algorithm are used to measure its strength.The Larger the key length;is the longer the data will be secure.Contrary to popular beliefs,Hashing is not a form of Encryption although it applies Cryptography in its functions.Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality,but also the following key **elements** of security:

Authentication: the origin of a message can be verified.
Integrity: proof that the contents of a message have not been changed since it was sent.
Non-repudiation: the sender of a message cannot deny sending the message.



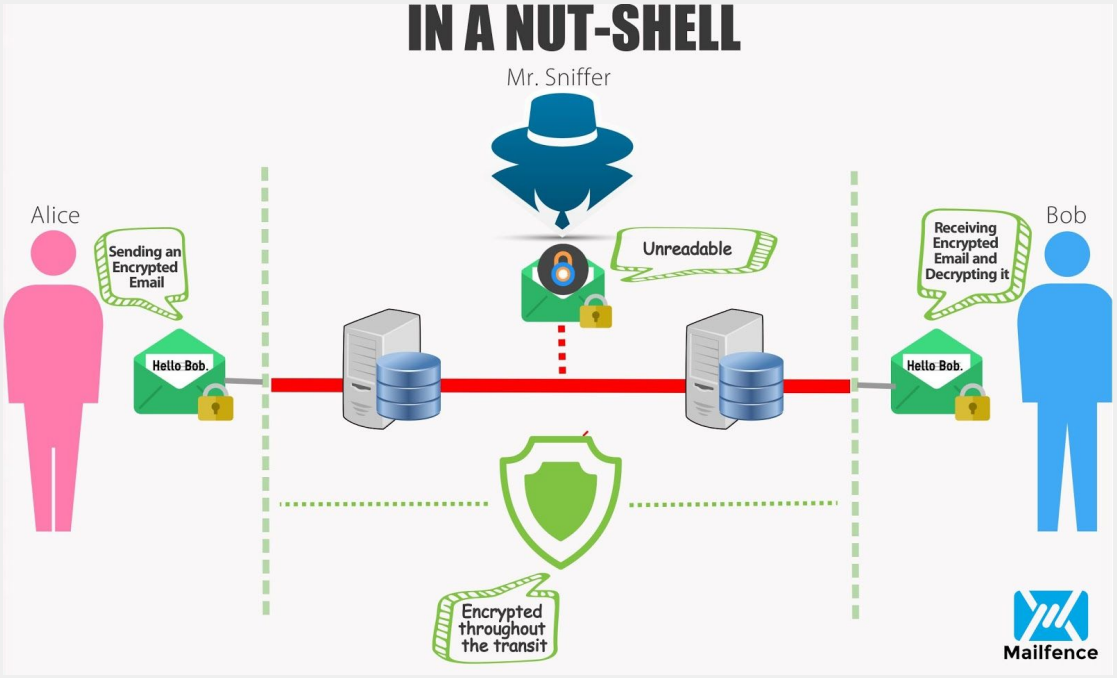
Cryptographic Hash- A cryptographic hash function or algorithm is one that takes an arbitrary block of data and returns a fixed-length string(**the hash**) in a way that any(accidental or intentional) change to the data will(with a very high probability)change the hash value.The data to be encoded are usually called the message and the hash value is sometimes called the 'message digest' or simply 'digest'.A hash function can also be said of as a piece of code that takes a piece of information and scrambles it up mathematically into a fixed-length piece of gibberish which is called 'hashing' the data.This hash is unidirectional and it makes it very difficult to get back the original message from the digest.It's very easy to take a piece of information and figure out its unique hash.It's very hard to take a hash and find a piece of information that generates it.In fact,if you use a random password, you have to try every possible combination in order to do it, which is more or less impossible.There should never be two messages with the same hash.'password' and 'password1' have very different hashes(**as different as night and day**).Moreover,a good hash function should produce totally different results if even a single character is changed.

Hashes have some really useful properties for password applications.When you sign up to a website and create an account,the password is stored as a hash and not as a plaintext.On the next login,the inputted password is hashed using the same hash function,and this new digest is compared to the one in the database;if they match the user gains access to his/her account.Instead of storing the password,you store the hashes of the passwords.It is vital that the actual plaintext passwords are never stored on the server.So,when hackers breach the server,they can't steal any passwords – only hashes.To crack a password,the hackers have to use the hashing algorithms to generate hashes and if they match with the hash obtained from the server,then they have successfully cracked the password.

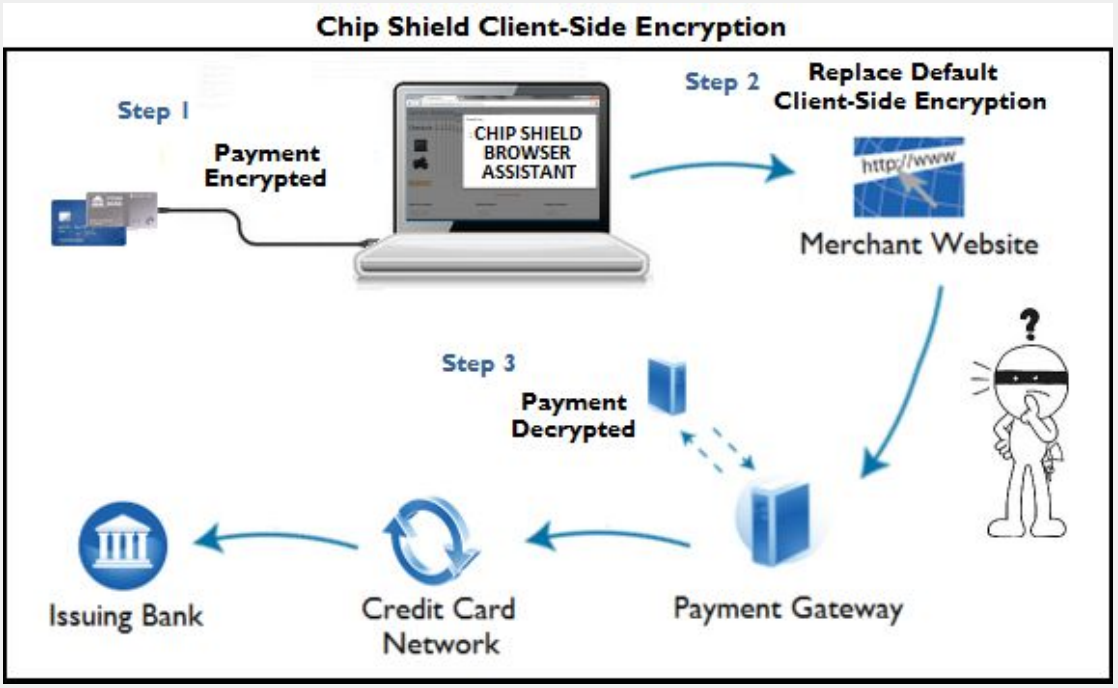
Emails,End-to-End Encryption vs Client Side Encryption In Relation to Passwords



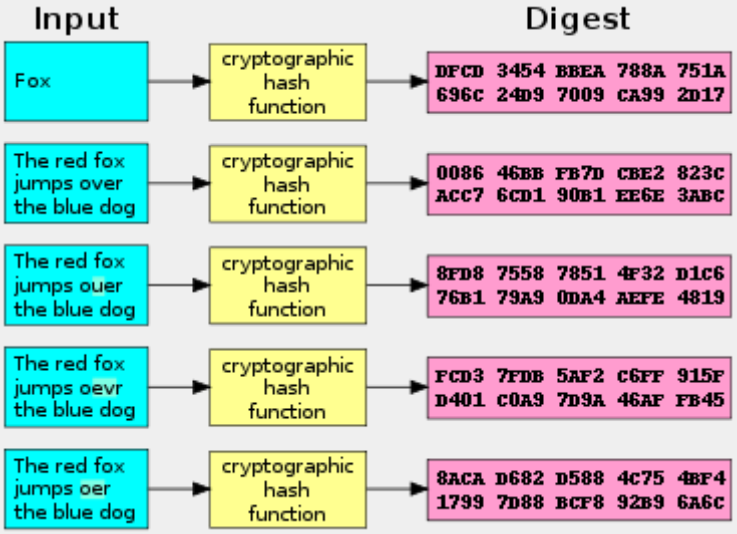
End-to-End Encryption is encrypting data at rest and keeping it encrypted in transit until it reaches the final destination,where decryption occurs.The main limitation of End-to-End Encryption is that it is not definitively clear what **"end-to-end"** actually means and largely affects the implementation of End-to-End Encryption.During the multiple transit stages through different **Applications** and **Operating Systems**;there are cycles of decryption and re-encryption which make the data very vulnerable.Tokenization technology is being viewed as a better alternative.If a password was in transit through end-to-end encryption.



Client-Side Encryption (CSE) is a technique that applies cryptography to encrypt files before they leave your PC to another destination.The major CSE algorithms are RSA and AES.The key to decrypt the file is usually stored on the client's computer.The main advantage of CSE is that since the decryption key is stored on your device,you are the only one who has access to your data.In the scenario that you lose your password, your service provider cannot help you retrieve it because they never had the access key or knew your password in the first place,which makes it imperative to have such data backed up on your own system.A majority of computers will work with CSE as long as computer itself is secure.On the other hand,smartphones have the computational power to perform CSE using the same technology that secures HTTPS connections for mobile phones.CSE also has drawbacks such as Forgetting Passwords,Reduced File Sharing Capabilities since only one party(the owner) has the decryption key for the data,it is therefore vital to be **aware** of the types of files and data that are protected with Client-Side Encryption.



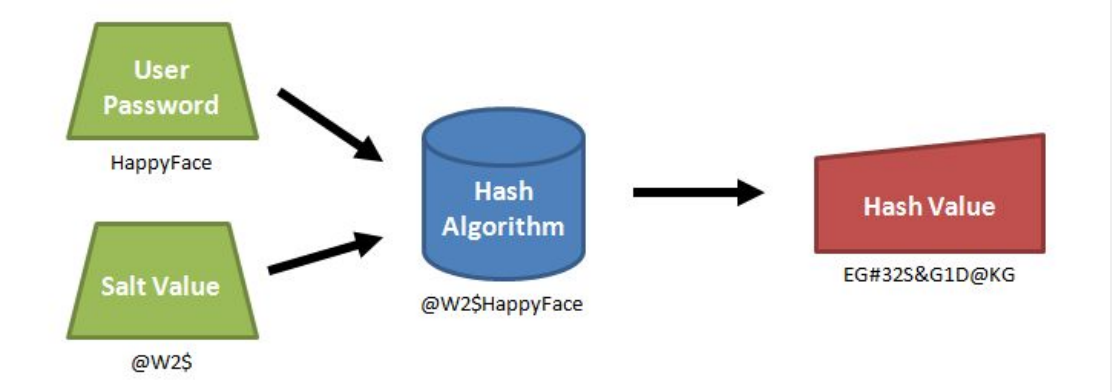
Hashing Algorithms





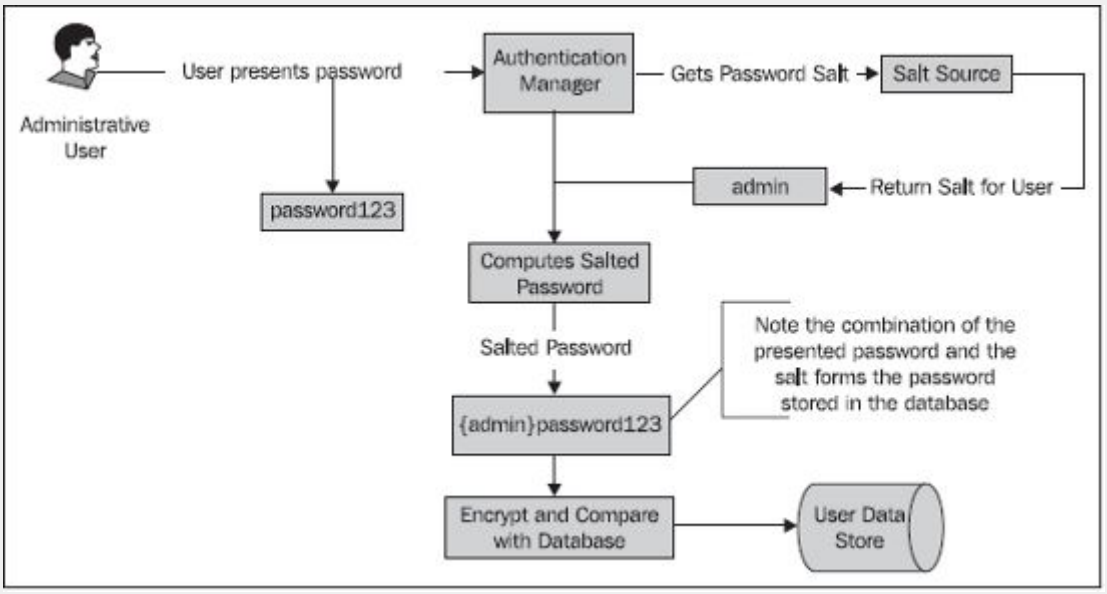
There are many hashing algorithms available but many of them are weak such as LM and **NTLM** for Windows Systems.Others are **SHA1,MD5** and

SHA3,**Blowfish**,**PBKDF2** and **Twofish**.During the many cases of data breaches,it has been discovered that these poor hashing functions are the ones that have been largely used.The best hashing functions are Bycrypt and Scrypt.For example using MD5 to generate the hash value for 'password' **will output>**"5f4dcc3b5aa765d1d8327deb882cf99" and 'password1' **will output>**"7c6a1180b3689a0a88C02787eeafboe4c".Notice the grave differences in the two hashes because of just one character we have added.**SHA512 Crypt** Function(similar to Bcrypt and Scrypt) included by default in **Mac OS X** and most **Unix-based** Operating Systems passes text through 5,000 hashing iterations/loops,which would limit the GPU cracking system to slightly less than 2,000 guesses per second.



Algorithm	Maximum Password Length	Length of Salt, base64	Iterations	Length of Hashed String, base64	Maximum Length of Hashed Password, base64
MD5	255	2 to 8-char (48bit)	1000 (built-in)	22-char (128bit)	37-char ({smd5}salt$hashed_str)
SHA1	255	8 to 24-char	2^4 to 2^{31} (cost is 4 to 31)	27-char (160bit)	62-char ({ssha1}nn$salt$hashed_str)
SHA256	255	8 to 24-char	2^4 to 2^{31} (cost is 4 to 31)	43-char (256bit)	80-char ({ssha256}nn$salt$hashed_str)
SHA512	255	8 to 24-char	2^4 to 2^{31} (cost is 4 to 31)	86-char (512bit)	123-char ({ssha256}nn$salt$hashed_str)
Blowfish	72	22-char	2^4 to 2^{31} (cost is 4 to 31)	32-char (192bit)	69-char ({ssha256}nn$salt$hashed_str)

Salts



These technique was designed to combat rainbow tables.Salting involves adding a bunch of random characters to the end of a password before hashing it.These extra characters are the ones called salts and by doing this we have a totally different hash which **won't** be in the rainbow table.The characters added are big,between 10-20 characters and would usually come in handy to protect users who use 4 or less than the largely **accepted** minimum of 8 character passwords.The server simply appends the salt to the user inputted password and then hashes it.The huge advances in GPU-assisted password cracking have diminished much of the advantages of rainbow tables,while salting has also greatly reduced the threat of rainbow tables.Salting appends several unique characters to each account password before running it through a cryptographic function,a process that blunts the value of rainbow tables and other types of precomputed attacks.The salt must be saved for each user and is usually stored beside the user name and password hash,so the information is available during each user login.Salt is rarely kept apart from the hash.Even when known,its virtue lies in its uniqueness,which defeats pre-computation of results.)



In addition to making rainbow-table attacks infeasible, salting can also significantly add to the resources required to carry out more traditional cracking attacks,since it ensures that each stored hash is unique even if two users choose the same passcode.That,in turn,requires each hash in a compromised table to be cracked separately even if they mask one or more

identical plaintext passwords.

Hashes derived from **NTLM**,because they **never** use salting,are among the easiest to crack.

One for the biggest mistakes websites make is not applying salting to passwords,which is substantially detrimental to the users.Websites and online services should also take care when using Salting because if they use the same salt for all the users,the attackers will be able to **create a rainbow table specifically for that particular website and this leaves the site highly susceptible to compromise**.Using random and unique salts for each user is the **best** option.

Password Cracking Tools



1)Cain and Abel
This is a very well known tool capable of handling a variety of tasks but is only available for **Windows** Operating System.It is interesting in the sense that it does not exploit any vulnerabilities or bugs but only covers security weaknesses of protocols to grab the password: Sniffing the network,cracking encrypted passwords using dictionary attacks,brute force attacks,cryptanalysis attacks,revealing password boxes,analyzing routing protocols and decoding scrambled passwords are just some of the exploits it can perform.It was developed with Network Admins,Penetration Testers,Forensic Experts and Security Professionals in mind.

2)John the Ripper
It is a free source password cracking tool available for **Windows**,**Linux**,**Unix** and **Mac OS X** Operating Systems.It's main strength is detecting weak passwords.Quite a very popular tool.

3)Aircrack-NG
A WiFi password cracking tool that can crack WEP/WPA protocols' passwords,by analyzing wireless encrypted packets and then tries to crack passwords based on its cracking algorithm.
Available for **Linux** and **Windows** Operating Systems.

4)Ophcrack
It is a Free rainbow-table based password cracking tool for **Windows**.It is

very popular for use with the **Windows** Operating System platform but it can also be used on **Linux** and **Mac** Systems.
It will crack LM and NTLM(both hashing functions based on the and built for Windows OS) password hashes.You can also find readily available free-rainbow tables for Windows OS variants i.e **Windows XP**,**Windows Vista** and **Windows 7**.

5)Lophtcrack
Built as an alternative to Ophcrack.It attempts to crack **Windows** OS password hashes.Uses **Windows** workstations,network servers,primary domain controllers and Active Directory to crack passwords.
Dictionary and Bruteforce attacking techniques are applied to generate and guess passwords.

6)Medusa
Medusa is a speed parallel,modular and login brute-forcing tool similar to THC Hydra.It supports a lot of network protocols from which to crack passwords; HTTP,CVS,AFP,IMAP,MS SQL,FTP,MY SQL,POP3 Amongst a host of others.

7)THC Hydra
A very fast network logon password cracking tool; available for **Windows**,**Linux**,**OS X**,**Solaris** and **Free BSD** platforms.When compared to other cracking tools,it is really fast,Largely owing to the fact that it supports most(**over 35 protocols**)if not all of the available network protocols;Asterisk,HTTP FORM-POST,HTTPS-FORM GET,CVS,Firebird,FTP,Cisco AAA,Cisco author,IMAP,LDAP,Cisco enable,XMPP,Telnet,SMTP,PCNFS,Rexec,Oracle Listener among others.

8)Wfuzz
It is a Web application password cracking tool that employs bruteforce attack to crack passwords.It can also be used to find hidden web resources like directories,servlets and scripts(e.g **JavaScript**).
Quite a powerful tool that can be used to identity different kinds of injections like SQL,LDAP and XSS in web applications to carry out injection attacks via multiple points with multiple dictionary leading to database compromise in website's servers.Its main other prominent features are:Bruteforce HTTP password,POST and GET Bruteforcing,Cookies fuzzing,Post,Website Headers and authentication data bruteforcing among others.

9)Brutus
A popular online password cracking tool available only for **Windows** Systems.It supports multi-stage authentication engines and is able to connect 60 simultaneous attacks(makes it effective in bruteforcing passwords because many are tested at the same time thus greatly reducing the workload and saving the attacker a lot of time).It supports most of the major networking protocols: IMAP,NNTP,NetBus,POP3,HTTP(Basic Authentication),FTP,Telnet,HTTP(HTML Form/CEIT),SMB etc.

What's more interesting and makes this tool even more popular amongst the attackers circles is that you can create your own authentication types and it has Resume and Load Options meaning that you can pause and resume the attack process at any time you want.

10)Rainbow Crack
A tool that mainly deals with Rainbow tables and is available for **Windows** and **Linux** Systems.It is basically a hash cracker tool that uses a large scale time-memory trade off process for fast password cracking than traditional Bruteforce tools.

*__Time-Memory trade off__ is a computational process in which all plain text and hash pairs are calculated by using a second hash algorithm. After computation,results are stored in the rainbow table which is very time consuming;but once the table is ready it will crack passwords quite faster than bruteforce tools.The developers have also generated rainbow tables for most of the weak password hashing algorithms; LM rainbow tables,NTLM rainbow tables,MD5 and SHA1 rainbow tables.Some of these tables are available free and others for sale- on it's official website.**Other tools are DaveGrohl and Elcomsoft etc.**

Online 'Hacker' Forums



The world has become a global village thanks to the internet and communication.People are constantly sharing information across the globe;whether good or bad.The same applies to hackers and cyber criminals.They do not operate in isolation,we have heard of hacker groups from some countries carrying out hacking exploits.What's more is that through the web there are a lot of resources that can assist them in their exploits e.g Over 2.5 billion passwords have been leaked and most of them are posted on various sites for everyone to see and try whatever he wants with them.

Witness Free Rainbow Tables- is a project that allows volunteers to donate spare computer cycles to generate publicly available tables that crack hashes returned by algorithms including SHA1,MD5 and NLTM.It's organizers have already amassed over 6 terabytes worth of data.Over 4000 volunteer computers participate;with 36 megabits of table data each second.Between 2011-2012 over 100 million passwords were published online as plaintext or ciphertext that can easily cracked.There is even an Annual Password Contest,dubbed 'Crack Me If You Can' where teams of great password crackers compete in who will cracking the most passwords availed for cracking- which is usually held at the **Defcon Hacker Conference**.The ever-growing list of leaked passwords allows programmers to write rules that make cracking algorithms faster and more accurate; password attacks have become cut and paste exercises that script kiddies(people who have little or no knowledge of hacking and just follow other expert hacker's methods)can perform it with ease.In fact anyone who is tech savvy and with no programming knowledge and provided with the tools can crack passwords.



Cracking 16 character passwords was not feasible at all 5 to 7 years ago but it

is a reality now,why?it is not the advent use of Supercomputers but more advanced techniques;the **OclHashcat** program(hacking tool developed by hackers) effectively uses GPU cards like the AMD Radeon HD7970 and HD6990 Cards(which as we have seen are very good at mathematical calculations and bruteforce attacking passwords).

After a LinkedIn leak of 6.5 Million password hashes,it took only 6 days to crack 90% of them.In another data breach,Back in late 2009,the Rock You.com site which is an online games service,was compromised through an SQL injection attack.Over 14 Million common plaintext passwords to the public and it within days,most of the password hashes had been converted to plaintext.The trend here is that most of the password hashes used are weak and poor such as MD5,SHA1 and LM/NTLM and because people are watching,sharing info and when they see an exploit;they'll be sure to carry it out.This would not have been the case a few years ago and the online services would have gotten away with it.

Rainbow Tables were conceived and almost instantly(perhaps overnight),the approach towards password cracking had drastically changed.Rainbow Tables are based on the Time-Memory trade off concept by Martin E. Heuman in 1980.He published a paper titled 'A Cryptanalytic Time-Memory Trade-Off' popularly known as **Heuman Tables**.Rather than the traditional way of asking a computer to enumerate each possible password in real-time and compare it against a targeted hash,which required many computing requirements(lot of storage space and memory).Heuman tables were alternatively different since precalculated data was stored in memory or on a disk in a highly compressed form to speed up the process ultimately lowering the computing requirements (**storage space and time**) needed to bruteforce huge numbers of hashes.**Hashlists** are dumped daily on www.pastebin.com and other sites.It is also possible to ascertain if your accounts have been compromised by visiting www.haveibeenpawned.com.

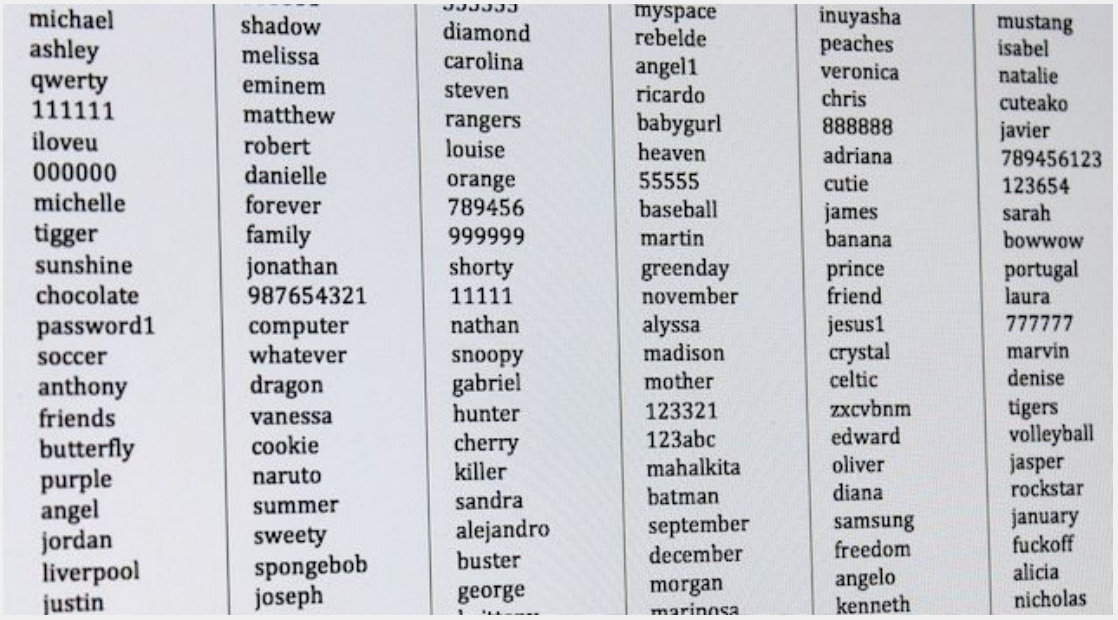
OpenWall.com



A website that has numerous password cracking resources.

1)It has more than 3546 entries of common passwords list by **Openwall Project**.The lists are based on passwords most commonly seen on a set of Unix Systems in the Mid-1990s,with more common passwords listed first.It also includes common passwords from public lists of passwords from major community website compromises that occurred between 2006 and 2010.

Wordlists



michael	shadow	diamond	myspace	inuyasha	mustang
ashley	melissa	carolina	rebelde	peaches	isabel
qwerty	eminem	steven	angel1	veronica	natalie
111111	matthew	rangers	ricardo	chris	cuteako
iloveu	robert	louise	babygurl	888888	javier
000000	danielle	orange	heaven	adriana	789456123
michelle	forever	789456	55555	cutie	123654
tigger	family	999999	baseball	james	sarah
sunshine	jonathan	shorty	martin	banana	bowwow
chocolate	987654321	11111	greenday	prince	portugal
password1	computer	nathan	november	friend	laura
soccer	whatever	snoopy	alyssa	jesus1	777777
anthony	dragon	gabriel	madison	crystal	marvin
friends	vanessa	hunter	mother	celtic	denise
butterfly	cookie	cherry	123321	zxcvbnm	tigers
purple	naruto	killer	123abc	edward	volleyball
angel	summer	sandra	mahalkita	oliver	jasper
jordan	sweety	alejandro	batman	diana	rockstar
liverpool	spongebob	buster	september	samsung	january
justin	joseph	george	december	freedom	fuckoff
			morgan	angelo	alicia
				kenneth	nicholas

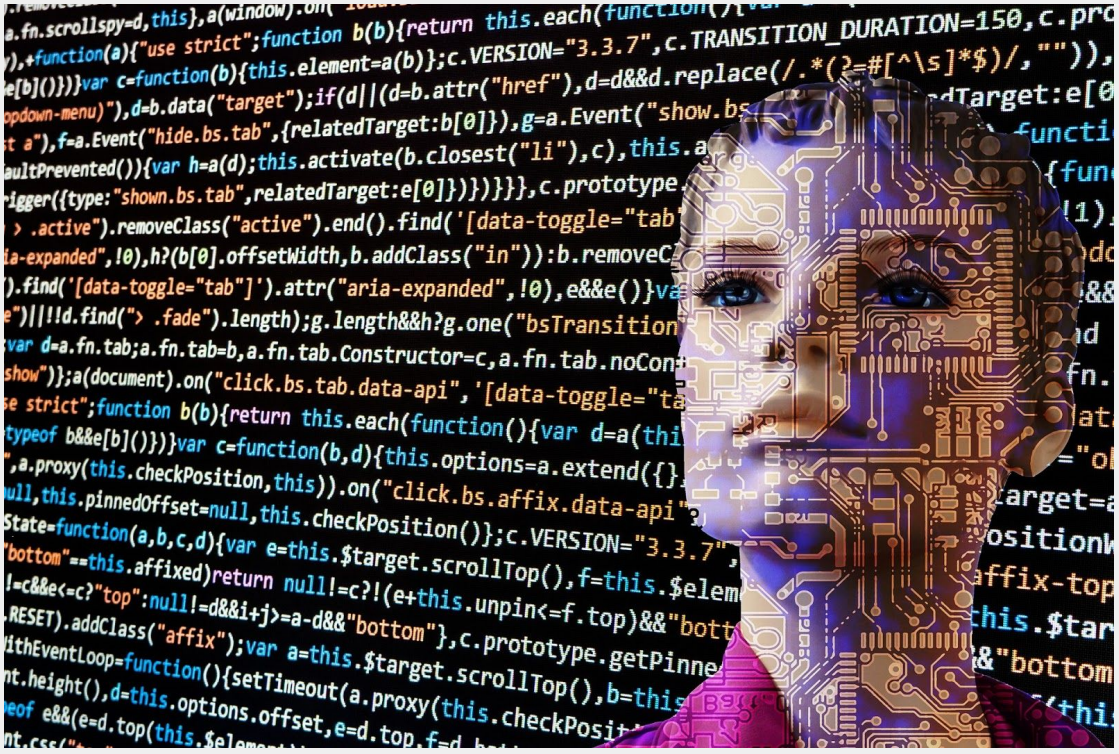
These are common words and password lists.Password wordlists are intended for use especially with tools like John the Ripper and other password cracking utilities via the Brute-force technique.They are based on human languages like:Afrikaans,Croatian,Czech,Hungarian,Dutch,English, Danish,Finnish,French,German,Italian,Japanese,Latin,Norwegian,Swedish,Swahili,Spanish,Russian and Yiddish.Common passwords and unique words from the available languages are also included in a list.All of these are combined in a file of 40 MB that has almost 4 Million Entries.Such a wordlist is sold for around $27.95.Its File Archives Include:
1)Public wordlists and their mirrors among other things.
2)A wordlist titled 'Uniqpass wordlist' going for $12.99,but there is a free preview of a cut-down wordlist.
3)Crackstation's password Cracking Dictionary-> 15 GB wordlist containing dictionary words,leaked passwords,words from **Wikipedia articles** and project **Gutenberg books.**

The word lists collection is a result of processing many hundreds of public domain wordlist files from multiple sites and in a variety of file formats(ensuring duplicates and poor quality files are punched).

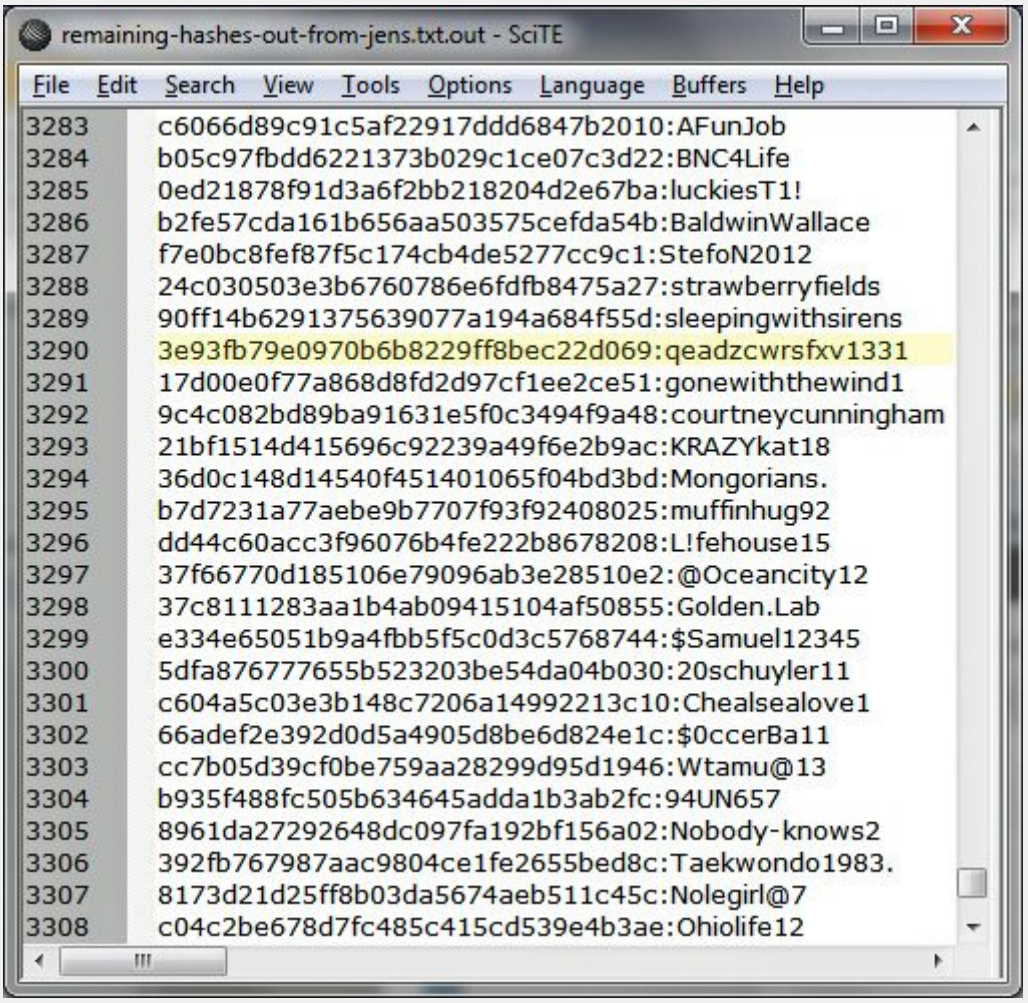
Included only in the full version and not available in the freely downloadable version of the collection is a huge list of all the common passwords and words from all languages with word mangling rules applied (to form other likely passwords,such as by adding capitalization or digits to words)excluding any duplicates.This wordlist is provided as a single text file->with over 40 Million entries and around 500 MB in Size.All wordlists are sorted either **alphabetically** or **for more common to less common** passwords/words/languages with alphabetical order within each section (for about equally common passwords/words or for individual languages).All these handful of sources of information and resources only make password cracking easier.It is easy to access this resources and anyone willing can be able to crack passwords. People should therefore stop being naive and stay

put,looking out for happenings that could impact their security and always staying on top of their game.

Anatomies Of Password Cracking



In a blog post written by ***Dan Goodin****,the security editor at* ***Arstechnica.com****,a technology blog dated 05/27/2013 at 8.00 am and titled Anatomy of a hack: "How crackers ransack passwords like "qeadzcwrsfxv1331" he details a hacking escapade involving a lot of many techniques and covers nearly everything there is to say about passwords,Read On some excerpts of the post:*



The list of plains contains "123456," "1234567," and "password" ,"letmein," "Destiny21," and "pizzapizza." Passwords of this ilk are hopelessly weak.Despite the additional tweaking, "p@$$word," "123456789j," "letmein1!," and "LETMEin3" are equally awful. But sprinkled among the overused and easily cracked passcodes in the leaked list are some that many readers might assume are relatively secure.":LOL1313le" is in there,as are "Coneyisland9/," "momof3g8kids," "1368555av," "n3xtb1gth1ng," "qeadzcwrsfxv1331," "m27bufford," "J21.redskin," "Garrett1993," and "Oscar+emmy2."....*

....What was remarkable about all three cracking sessions were the types of plains that got revealed.They included passcodes such as "k1arajohnson," "Sh1a-labeouf,""Apr!l221973,""Qbesancon321,""DG091101%,""@Yourmom69," "ilovetofunot," "windermere2313," "tmdmmj17," and "BandGeek2014." Also included in the list: "all of the lights" (yes, spaces are allowed on many sites), "i hate hackers," "allineedislove," "ilovemySister31," "iloveyousomuch,""Philippians4:13","Philippians4:6-7,"and"qeadzcwrsfxv1331"."gonefishing1125" was another password Steube saw appear on his computer screen. Seconds after it was cracked,he noted,"You won't ever find it using brute force."

Dictionary lists, hybrid attacks and mangle rules

```
#define RULE_OP_MANGLE_LREST            'l' // lower case all chars
#define RULE_OP_MANGLE_UREST            'u' // upper case all chars
#define RULE_OP_MANGLE_LREST_UFIRST     'c' // lower case all chars, upper case 1st
#define RULE_OP_MANGLE_UREST_LFIRST     'C' // upper case all chars, lower case 1st
#define RULE_OP_MANGLE_TREST            't' // switch the case of each char
#define RULE_OP_MANGLE_TOGGLE_AT        'T' // switch the case of each char on pos N
#define RULE_OP_MANGLE_REVERSE          'r' // reverse word
#define RULE_OP_MANGLE_DUPEWORD         'd' // append word to itself
#define RULE_OP_MANGLE_DUPEWORD_TIMES   'p' // append word to itself N times
#define RULE_OP_MANGLE_REFLECT          'f' // reflect word (append reversed word)
#define RULE_OP_MANGLE_ROTATE_LEFT      '{' // rotate the word left.  ex: hello -> elloh
#define RULE_OP_MANGLE_ROTATE_RIGHT     '}' // rotate the word right. ex: hello -> ohell
#define RULE_OP_MANGLE_APPEND           '$' // append char X
#define RULE_OP_MANGLE_PREPEND          '^' // prepend char X
#define RULE_OP_MANGLE_DELETE_FIRST     '[' // delete first char of word
#define RULE_OP_MANGLE_DELETE_LAST      ']' // delete last char of word
#define RULE_OP_MANGLE_DELETE_AT        'D' // delete char of word at pos N
#define RULE_OP_MANGLE_EXTRACT          'x' // delete X chars of word at pos N
#define RULE_OP_MANGLE_INSERT           'i' // insert char X at pos N
#define RULE_OP_MANGLE_OVERSTRIKE       'o' // overwrite with char X at pos N
#define RULE_OP_MANGLE_TRUNCATE_AT      '\''// cut the word at pos N
#define RULE_OP_MANGLE_REPLACE          's' // replace all chars X with char Y
#define RULE_OP_MANGLE_PURGECHAR        '@' // -- not implemented --
#define RULE_OP_MANGLE_DUPECHAR_FIRST   'z' // prepend first char of word to itself. ex:
hello -> hhello
#define RULE_OP_MANGLE_DUPECHAR_LAST    'Z' // append last char of word to itself.   ex:
hello -> helloo
#define RULE_OP_MANGLE_DUPECHAR_ALL     'q' // duplicate all chars. ex: hello ->
hheellllloo
```

Read the full post here>https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/3/



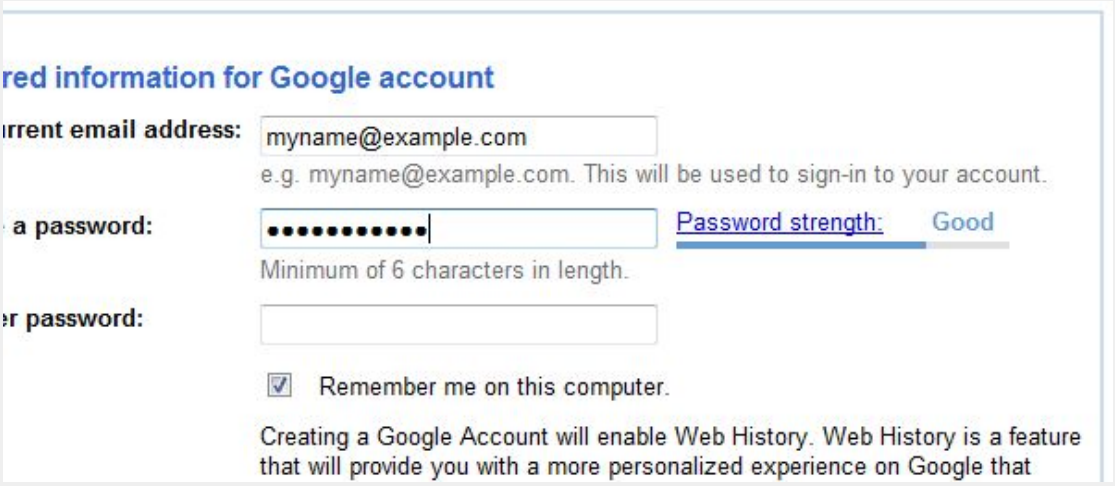
*In yet Another blogpost still by **Dan Goodin** and **ArsTechnica**,dated August 21,2012 at and titled 'Why Passwords have never been weaker- and crackers have never been stronger';he gives more insight into passwords and password cracking….*

Passwords such as "mustacheehcatsum" (that's "mustache" spelled forward and then backward) may give the appearance of strong security,but they're easily cracked by isolating their patterns,then writing rules that augment the words contained in the RockYou dump and similar lists.For Redman to crack "Sup3rThinkers", he employed rules that directed his software to try not just "super" but also "Super", "sup3r", "Sup3r", "super!!!" and similar modifications.It then tried each of those words in combination with "thinkers", "Thinkers", "think3rs", and "Think3rs".That subtlety takes all sorts of forms...The hybrid is my favorite attack," said Atom, the pseudonymous developer of Hashcat, whose team won this year's Crack Me if You Can contest at Defcon."It's the most efficient.If I get a new hash list,let's say 500,000 hashes, I can crack 50 percent just with hybrid."

Read the full post here>https://arstechnica.com/information-technology/2012/08/passwords-under-assault/

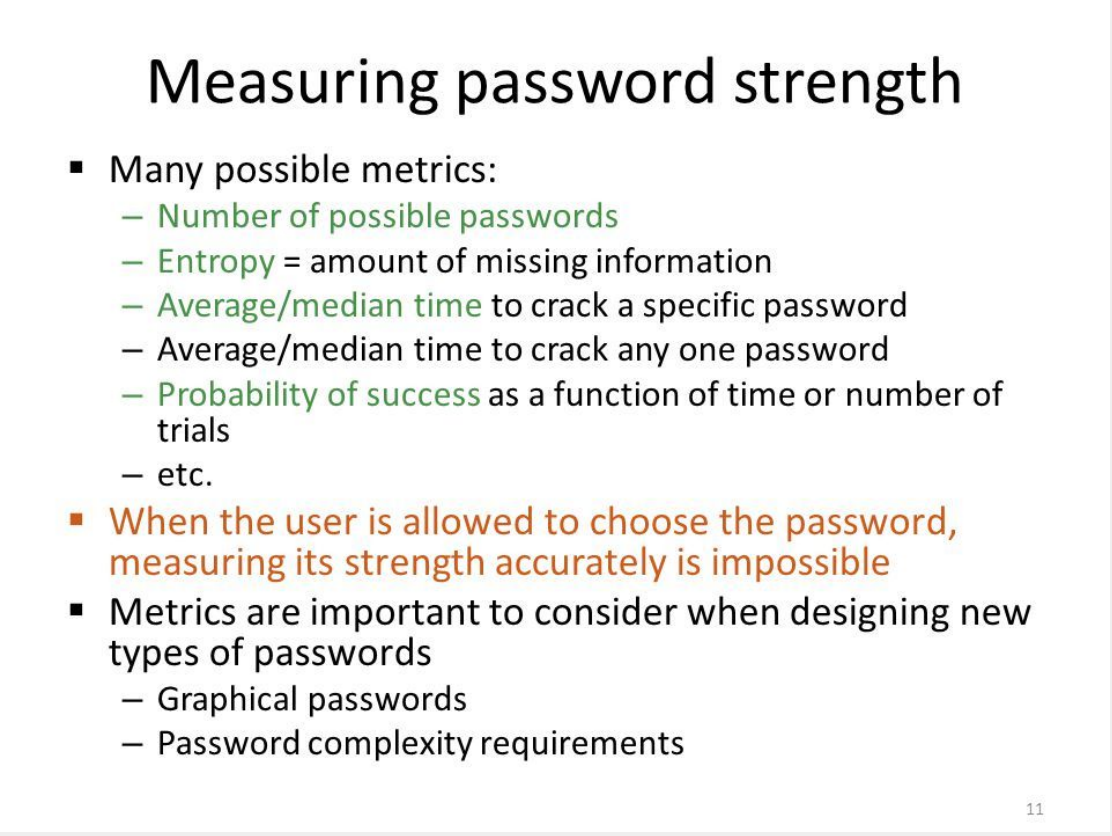
4] Secure Techniques

Password Length and Strength



Weak authentication security is the leading cause of data breaches.This has been **proven time and again**.Lengthy passwords are often associated with an increase in entropy.Entropy is the randomness collected for use in cryptography (the science of encryption) or other uses that require random data.An increase in entropy is seen as Directly proportional to password strength.When cracking passwords,keyspace is used to determine and calculate the strength of the password.**Keyspace** relates to character sets (**a-z,A-Z,0-9,symbols and Unicode symbols that look like numbers**)

available on the standard keyboard of a PC or Mobile Phone and other devices.For example,an 8 character password containing only lowercase letters which are 26 in number therefore has a keyspace of 26^8,the power is the character length of the password and in this case the length is 8 characters.If you consider both uppercase and lowercase letters they are 52 in number therefore a password of 8 characters has a keyspace of 52^8.The main method of cracking these passwords is through Brute force attack (**Discussed in chapter 4**).Using Brute Force attacks to crack the password elvis2017 would require 62^9 possible combinations.The keyspace of 62 has been arrived at by the number of possible letters i.e uppercase and lowercase plus the number of numerals(0-9) and to the power of 9(the password character length).Graphical Processing Cards have a lot of computing power than the normal CPUs;that is mathematics,physics and even Artificial Intelligence.This has made GPUs very popular specifically the AMD Radeon 7970 and the AMD Radeon HD 6990.If the attacker only used AMD Radeon HD 7970 about 19 days to churn through all the possible password combinations for our sample password elvis2017.However,if you incorporate features that are built into password cracking apps such as **Hashcat** and extreme GPU Brute force; the same password elvis2017 can be recovered in less time to around 90 seconds by performing a **Mask Attack**.



A Mask Attack works by intelligently reducing the keyspace to only those guesses likely to match a given pattern.It will not try kkkk1111,qqqqqq3333 and any other possible combination in between,instead trying a lower or upper-case letter only for the first character,and tries only lowercase

characters for the next four characters.It will then append all possible combinations in between,thus trying a lower or uppercase letter only for the first character,and tries only lowercase characters for the next four characters.All possible four-digit numbers are appended towards the end resulting in a drastically reduced keyspace of about 237.6 billion(**broken down into** 52*26*26*26*10*10*10*10).

Hybrid attacks are more powerful (**discussed in detail in chapter 4**).Hybrid attacks combines a wordlist,with rules to greatly expand the number of passwords those lists can crack.Hackers using this method will therefore not try bruteforce the five letters in elvis2017 but will rather compile a list of First Names,For each and every Social Network user e.g **Facebook** and **LinkedIn** and then adding them to a medium-sized dictionary of say,100 million words.The technique still requires more combinations than the mask attack-a lot of possible strings which can even be in the range of Trillions.Using the AMD Radeon HD 7970 Card will handle these large numbers in about two minutes.Similar passwords will also be easily cracked.

Security experts advise on passwords of a **minimum length** of around 14 and 20,that means that the keyspaces would be 26^14/52^14 or 95^14 if you check all the letters,numbers and symbols available on a standard English-Language keyboard.That being said,The maximum length depends on the ability of the user to recall such a password and the maximum possible length a system can handle.Using lengthy passwords poses problems to even powerful computation engines.Bruteforce attack like many other computational related techniques suffer from exponential growth i.e the more the figures to be calculated,the more time it takes to accomplish the task and submit the results,therefore even adding one more character makes the task more difficult.This does **not** mean that a lengthy password will never be cracked but it makes the password cracking task harder and take more time.Lengthy passwords,up to date information and good password policies will make the user more secure.

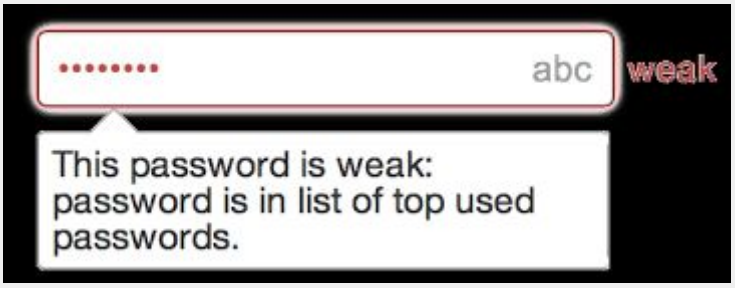
There have been dilemma as to whether short passwords of between 4 to 6 characters with a wide variety of characters are more secure than having a long password i.e Passwords like:

1){^q™7!
2)™^9!7)
3)3-©*•C
4)©=3°%]

For starters,a good password should have a wide variety of characters so that a password cracker will have to accommodate all the characters in a keyboard e.g 103^4 or 103^4...which is not mathematically a bigger number than 103^8or 103^13.In case the password only contains lowercase and uppercase characters;52^8 is still a bigger number than 103^4 or 103^6.The short passwords with a wide variety of characters will be cracked faster than longer

passwords with a minimal variety of characters or longer passwords with a wide variety of characters.**Use longer passwords all day,any day and if you use a wide variety of characters the better**.

Reference To Password Blacklists



A Password Blacklist is a list containing passwords that are commonly blocked and from use.They are passwords revealed from previous attacks,data breaches or which studies have shown to be weak,following common patterns or being easily guessed e.g Password1 and Shift123.They can be retrieved from readily available resources on the web and a simple google search will provide you with a list(s).Before selecting a password I suggest spending some of your time to view some of the blacklists since they can guide you and show you some of the trends to avoid(you know the drill,just google it!)Avoid using passwords that fall in worst password list.Every year,Data Analysis Companies publish the list of worst passwords of the year from analyzing all the leaked password's .Password blacklists should be incorporated to Password Policies.

The following is a list of the top 11 worst passwords of 2012**(globally)**:



(i) password
(ii) 123456
(iii) 12345678
(iv) abc123
(v) qwerty
(vi) monkey
(vii) letmein
(viii) dragon
(ix) 111111
(x) baseball

(xi) iloveyou

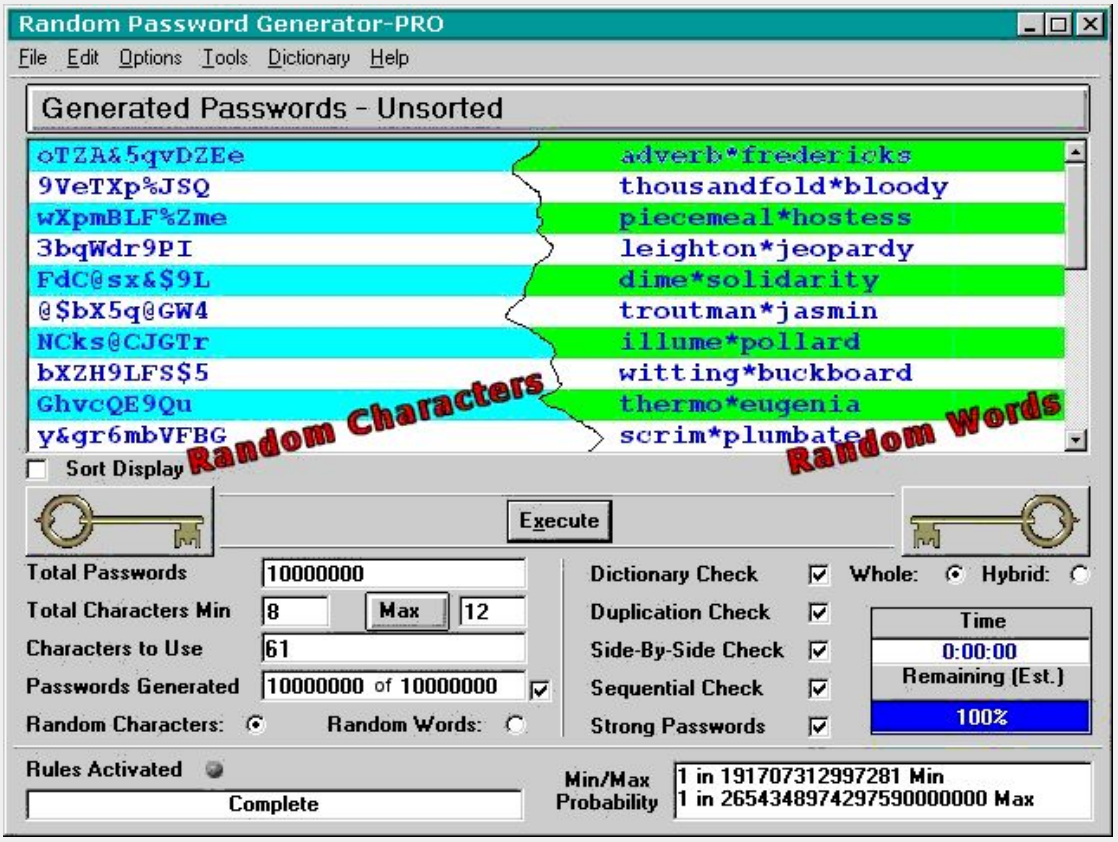
Careful Capitalization



Initially,adding many different character types was a ploy to expand the number of characters the attacker will have to go through whilst testing your password.**However,newer tools and techniques easily bypass this**.On a standard keyboard;
Small Alphabets: 26 Characters
Symbols: 33 or more.
Numbers: 10
I've seen misleading statements like "**If you add even one single Capital alphabet, the attacker will be forced to test another 26 characters**".This isn't entirely true because password cracker tools like OclHashcat have password mangling tools to be used in the Brute force attack.**This means that if the lowercase characters don't pass as the password;they are replaced with uppercase characters irrespective of where they are positioned on the password**.

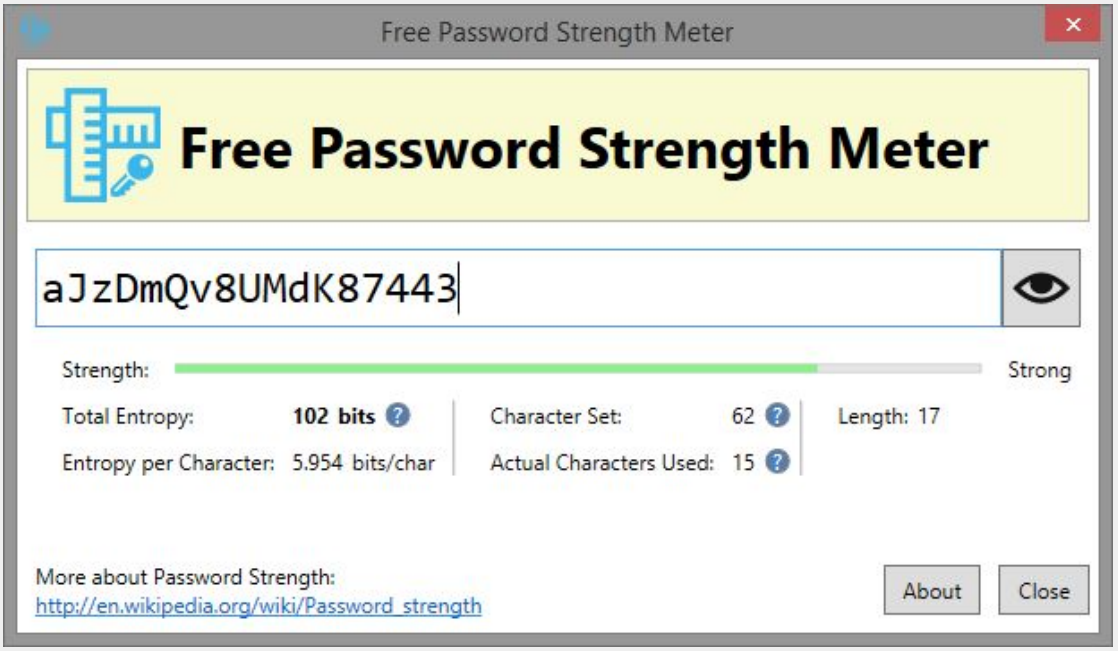
Example:let's use WiSpAuSu as our sample password.
And Let's Capitalize:
i) UsuapsiW/usuApsiW x
ii)usuApsiw/usUapsiw x
In example (i)the password and its variations is weak and not recommended because you have capitalized the first and last characters which is quite a common practice (ii)you have not capitalized the peripheral characters but using Mangling rules in bruteforce attack,the lowercase letters will be replaced by uppercase characters and vice versa for all the characters making up the password;until the password is cracked (iii)According to a diy attack,the components of the password follow a pattern of one or two digits i.e usu,uap,siw.

Random Password Generators

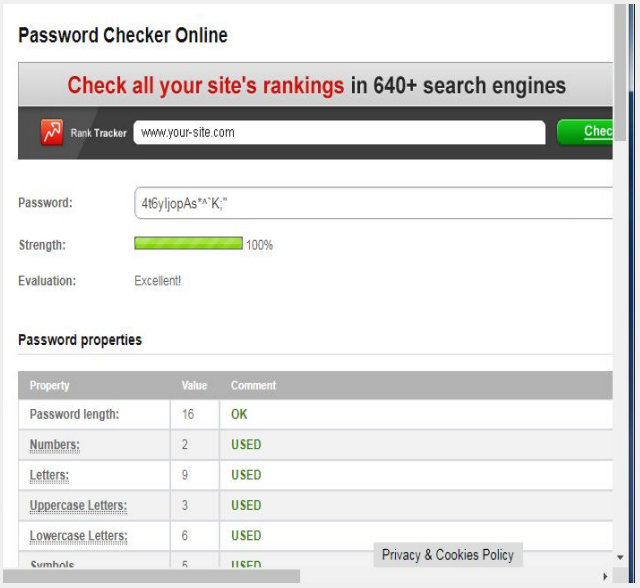


We have already talked about random things and that you should avoid real words.Random Passwords consist of symbols of specified length taken from some set of symbols using a random selection process in which each symbol is equally likely to be selected(**remember probability mathematics?**).The symbols can be individual characters from a character set,syllables designed to form pronounceable passwords,or even words from a wordlist,thus forming a **Passphrase**(a combination of real words to make a Password e.g 5 words).The strength of random passwords depends on the actual entropy of the underlying number generator;however,these are often not truly random but pseudo random(not fully random).Many publicly available password generators are found in programming libraries but they offer limited entropy.Most modern Operating Systems offer cryptographically strong random numbers that are suitable for passwords generation.Ordinary dice can also be used to generate random passwords.Random password programs **often** have the ability to ensure that the resulting password complies with a set local password policy;such as always producing a mix of letters,numbers and special characters.There are also web based Random Generators.They are also created to do all the work on the client's side i.e via JavaScript in the user's browser and the **password is never transmitted** to the Random Generator's server.

Password Strength Checkers

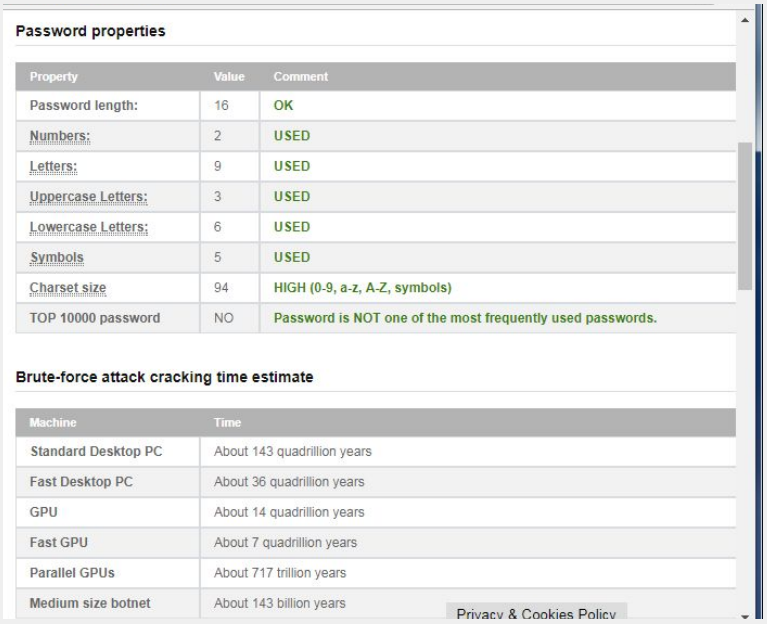


There are tools available on the web where you type in your password and they check it's strength based on certain criteria and properties.**Password Checker Online** is a good example of such tools.It attempts to be as helpful and transparent as possible on the **properties** that indicate the password strength;by analyzing the **syntax** of your inputted password and informs you about its **possible weaknesses**.The description of the site states that it is very **safe,and can be trusted**.This is because when you type your password to the password field,its syntax is analyzed on the client side(your side) by the JavaScript in your browser and under no circumstance is the password transferred over the network to their server.Being that they use the total number of combinations required in a brute-force attack to gauge a password's strength,we have to try and look at the downside;these meters fail to account for the patterns people employ to make their passwords memorable and which in turn frequently lead to passcodes that are **highly** susceptible to much more efficient types of attacks like **Hybrid Attacks**(especially **Markov Attacks**).



The password is checked against two main modes of password cracking:

(i)**Dictionary Attack -** Here the password is sent to their server in an encrypted form,leaving little or no chance for sniffing on the network, However,there is no protection against Man-in-the middle attacks(**via browsers**).A score of 0% to 100% is given to each password that the user selects.This score computation is mostly based on on the time that a middle-sized botnet(a PC that has being compromised to spread malware or perform other exploits without the knowledge if the user) would need in order to crack your password if it employs the brute-force attack.If the password is among the list of 10000 most common passwords - the password receives a score of 0 because this is deemed as too weak considering they are billions of passwords in the universe;10000 is not even a thousandth of a billion!The password checkers cannot evaluate and give a score computation if the password is made up of names or details about the system in which it is used.



Password properties

Property	Value	Comment
Password length:	16	OK
Numbers:	2	USED
Letters:	9	USED
Uppercase Letters:	3	USED
Lowercase Letters:	6	USED
Symbols	5	USED
Charset size	94	HIGH (0-9, a-z, A-Z, symbols)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 143 quadrillion years
Fast Desktop PC	About 36 quadrillion years
GPU	About 14 quadrillion years
Fast GPU	About 7 quadrillion years
Parallel GPUs	About 717 trillion years
Medium size botnet	About 143 billion years

Privacy & Cookies Policy

To compute the score,the following password properties are considered:

(I)The Length

(II)How many numbers used

(III)Uppercase letters

(IV)Lowercase letters

(V)Symbols

(VI)Charset Size (a-z,A-Z,0-9,symbols,Unicode class letterlike symbols).It would be good to exercise caution when using such meters.Never use passwords generated by them,but you should use them to guide you a bit on proper password generation techniques.

Password Managers



These are programs that assist in generating,storing and retrieving complex passwords from an encrypted database.With a password manager,you **won't need** to remember unique,long,complex passwords for every online account. The software will remember it for you, strengthening your password security and minimizing your risk the next time there's a massive data breach. All you'll need to remember is the single "master" password to the password manager itself.These programs typically require a user to create and remember one "master" password to unlock and access any information stored in its database i.e other passwords.The encrypted database is either stored locally on the user's device or stored remotely through an online file-hosting service.However,this depends on the type of password manager being used and its functionality as designed by its developers.



A researcher at the **Carnegie Mellon University** in 2014 found out that whilst browsers refuse to autofill if the Protocol on the current login page is different from the Protocol at the time the password was saved,some password managers would insecurely fill in Passwords for the http version of https-saved passwords.He also alleges that most managers did not protect

against iFrame and redirection based attacks and exposed additional passwords where Password Synchronization had been used between multiple devices.A strong password manager will oftentimes include a limited number of false authentication entries allowed before the password manager is locked down and requires IT services to be reactivated.Password managers should be used to generate long,random passcodes that are unique to each site.This is by far,the best way to protect against the brute-force attack and such passwords are the hardest to recover.There are even password managers which include a password generator.However,the password should be a cryptographically secure one to avoid generated passwords from being **susceptible** to compromise i.e if the password manager uses a weak random number generator...in which case a password could be guessable.

Types Of Password Managers:

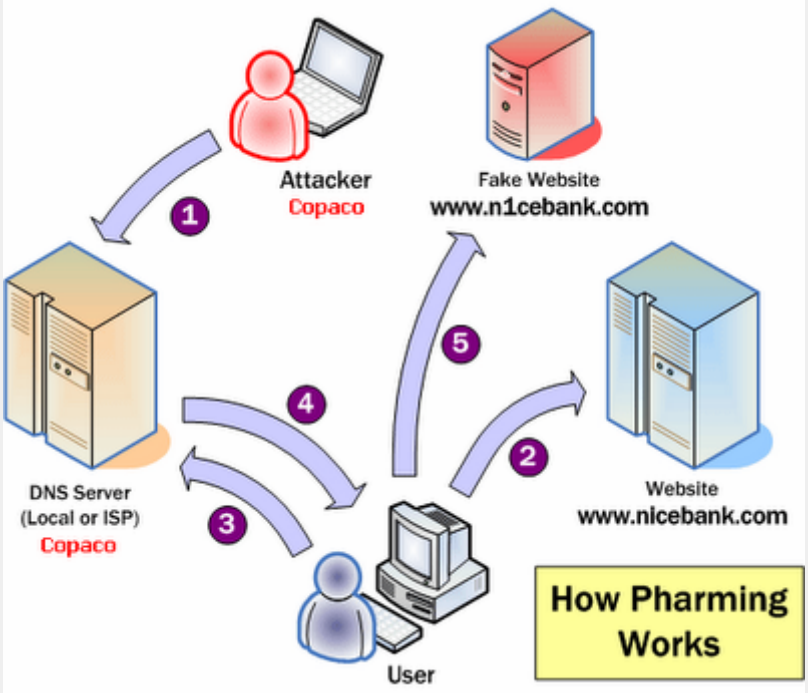
1)**Locally Installed Software-** Stored on the user's Mobile Devices e.g Smartphone,a Personal Computer in the form of a locally installed software application.These ensure that the password never reaches the web/internet,on its downside however,it can be quite a hassle to synchronize the vault with other devices.A good example of such a Password Manager is **Keepass**.

2)**Web-based Services/Cloud-based Storage-** A website that securely stores login details;a kind of an Online Password Manager.They are a web based version of more conventional desktop-based password managers.These password managers keep encrypted copies of your vault on their own servers and make sure all your devices are always synced.However,the disadvantage of cloud-based services is that if one of the services has been compromised and your passwords therefore leaked(**although the risk is small**).Examples of these Password Managers are **Last Pass**,**Dash Lane**,**Keeper** and **True Key**.

3)**Token-based hardware device -** These are locally accessible hardware devices,such as Smart Cards or secure USB Flash Devices**.**

It is important to note that **Sticky Password** and **1 Password** can work as **Device-based** or **Cloud-based**.Password Managers aim to solve the problems of human-generated passwords.They can also protect against **Phishing**(The act of attempting to acquire information and personal details such as passwords and usernames from people by masquerading as a genuine online service or website while in fact it's fake) and **Pharming**(A fraudulent practice of directing Internet users to bogus websites that mimic the appearance of a legitimate one,with the goal of obtaining personal details like passwords and usernames.Malicious code used to carry out pharming might be installed on PC or Web Server).Password Managers also incorporate an automated login script that first compares the current site's URL to the stored site's URL.In the event that the two don't match,then the password manager does not automatically fill in the login details.This measure aims at blocking visual imitations and look-alike websites.Many newer password managers

can handle complex passwords,multi-page fill-ins and multi-factor authentication.They are beneficial in automatically handling the more complex login procedures imposed by banks through online banking or just accessing their websites.Password Managers have also being proven to protect against keyloggers and other kinds of spyware.Through the use of multi-factor authentication,the password manager automatically fills in the details in the login fields,thus the user does not have to type any user credentials such as a username or passwords for the keyloggers to pick up.On the downside,however Password Managers cannot protect against man-in-the browser attacks,where malware on the user's device performs operations e.g on a banking website while hiding the malicious activity from the user.



Not everyone has been impressed by password managers though and various high-profile websites have **attempted** to block them.The reasons cited include:

I. **Compatibilty issues**
II. **To Protect against phishing**
III. **As a way of Blocking malware**
IV. **Protecting Against Automated Attacks**
V. **They are easily incorporated in most APIs available in many software products.**
VI. **Users are already familiar with the use of Passwords**
VII. **They require no extensive computer-server modifications.**

People should be very careful and cautious about the security standards because the databases of these programs can also be hacked and passwords for a lot of other accounts stolen.

Password Safe



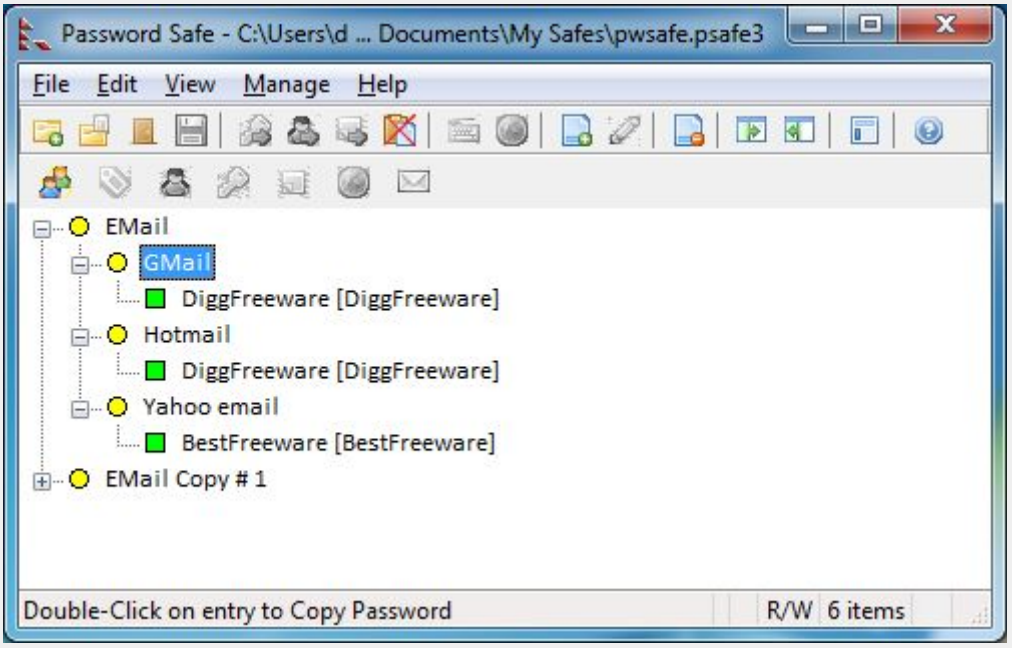
It is probably the most common and high level password manager program out there.It is a free and open-source program for use with Microsoft Windows.A beta version of it is also available across various Operating System variations such as **Ubuntu**(The Xubuntu and Kubuntu derivatives) and even **Linux.**A **java-based** version can be found on Source Forge; here you can find links to unofficial releases running on **Android**,**Blackberry** amongst other Mobile Operating Systems.The Password Safe was originally authored by **Bruce Scheiener** and developed by **Tony Shapiro Volunteers**.The Market release was on January 15,2002.(http://sourceforge.net/p/passwordsafe/-members).As of July 5,2017, the latest Windows version is 3.43.0.

Specifications;
1)Written in C++ Language but support's Ms Windows, Android,Linux(beta).
2)Size - 12 MB
3)Languages - 17
4)License - Artistic License 2.0

The official website is Password Safe.

The Interface is quite simple and intuitive,allowing users to set up their password database in minutes.The user need only recall a master password,once he fills it in;he can now access all account data entered and saved previously.The data can be organized by categories, searched and sorted based on references which are easy for the user to remember.Double Clicking and Pasting a Password into an application is a common activity here;The key combination of Ctrl+C copies the password or a selected account into the **Clipboard**, Ctrl+U copies the User ID.The program can be set to minimize automatically after a period of idle time and clears the clipboard.The stored passwords are then sectioned into groups and subgroups in a tree structure or

databases.It is even possible to compare and synchronize two different password databases.Changes to entries can be tracked,including a history of previous passwords,the creation time,modification time,last access time,and expiration time of each password stored.The software features a built-in password generator that generates random passwords.The user may also designate parameters for password generation(such as Length,Character set etc),therefore creating a "**Named Password Policy**" by which different passwords can be created.



When it comes to encryption,the password safe was initially built on Bruce Schneier's **Blowfish Encryption** algorithm.Two Fish encryption was instead implemented by Rony Shapiro along with other improvements to the 3.X.X version/series of password safe.(wineHQ).Two fish algorithm is a fast and free alternative to **DES Encryption** Standard.**CounterPlane Labs** under the supervision of **Bruce Schneier** have thoroughly verified the security of the Program.

Best Password Managers:

1)Last Pass

Billed at $12 per year.Last Pass can entirely live in your browser.

2)True Key

Billed at $20 per year and offers **6** different authentication factors including Facial Recognition and Fingerprint Scanning.

3)Dash Lane

Billed at $40 per year. It allows the user to reset all your passwords at once.

4)Keeper

Billed at $30 per year.It has a fast and robust interface.

5)Sticky Password
Billed at $30 per year.It offers **Local** or **Cloud-based syncing**.

6)KeePass
It is a Free Password Manager,the oldest,powerful and most challenging one to use;because you have to do everything yourself; be it learning how to use the program itself or even syncing,it is therefore best suited for more tech savvy people.

7)1 Password
Billed at $36 per year.It is available for **Mac,Windows** and **Android** Platforms.It has great form-filling abilities but lacks **true Two-Factor Authentication**.Recently,changes have been made to the effect that it is no longer possible to use **Local-Vaults** for Storage of Passwords.

Password Longevity/Duration

As seen when we discussed Password Policy,a good system should change a password as a precautionary measure or if the user believes the current password might have been compromised.Identity management systems are increasingly used to automate issuance of replacements for lost passwords;self-service password reset.The user's Identity is verified by asking questions and comparing the answers to ones previously stored (**when the account was opened**).Processes of password reset should be done through an automatic system and should not necessitate help from a customer assistant but not through emails or text or any other third party app.First of all,sending passwords via text or email is a totally bad idea because of social engineering and phishing vulnerabilities.As we saw in **Chapter 2(On Security Questions)**...self-service password reset saves the companies a lot of money.The integrity of the whole process is lost because the attacker gets a hold of the new password even before it is installed in the password database.Some password reset questions ask for personal information that could be found on Social Media(**Security Questions as we discussed in Chapter 2**).Password longevity is mainly aimed at trying to cut down the time an attacker would need to succeed in cracking the password.In the past years,the time needed to crack a password was estimated to be in terms of **Days,Months or even Years**.Nowadays,password cracking tools and GPU cards crack passwords in a matter of seconds,so this might not be as effective nowadays.



Password Duration also has its **drawbacks** because if a password has been compromised; it will be used immediately and trying to change it after it has already happened won't make a difference.If one has a really strong password,trying to change might be counterproductive because there is a risk that the new password selected will be less strong.

Personal Password Policy

A brute-force force attack is more likely when your Password protected PC is stolen,which is largely because most computers don't have any function to protect them from a brute-force attack.It is usually obvious that once someone has your computer,it's only a matter of time before they figure out your password.

(I) Pay Attention- To data breaches,happenings and events.Big corporations will inform clients soonest of data breaches and if you keep upto date you w(I)To protect yourself from brute-force attacks against online accounts,using strong passwords(as we've already discussed) is the way to go.Change passwords periodically - each 6 months or less if you're afraid an attacker might be able to catch up to you.

(II)Setup Automated backups for your PC(maybe weekly or fortnightly but I don't recommend monthly).You could even talk to an IT Professional about setting up your system to automatically erase itself after a certain number of failed login attempts.

(III)Use Unique Random Passwords- Usually by using Trusted and Secure(underline that)Password Managers especially Password Safe.Most password managers have the random password generators and because random passwords make it harder for automated tools to recognize when they've successfully cracked your password.This is an added layer of security.

(IV)Change Passwords Periodically-Security Experts advise changing passwords 3-6 months on critical accounts i.e(Banking,Email,Social Media and Anywhere you store backups e.g Clouds and Cloud Services) and yearly on non-critical accounts.

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\sneha>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.
```

(V)Users should not use autosave features to save passwords on their web browsers nor save passwords in plaintext form in their desktop files.If someone gets a physical hold of the machine or through other techniques such as spyware and malware,the accounts will be compromised

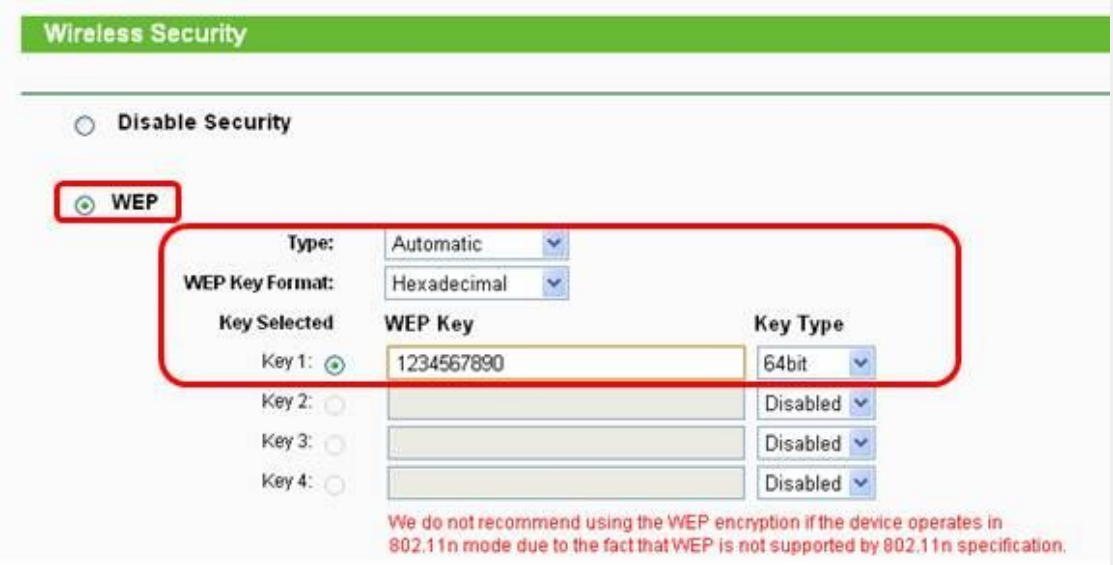
In the past few years,over 20 million passwords and usernames have being leaked,by doing research on the web you may bump into your own username or Password! and if not,since we have seen that passwords show a surprising degree of similarity;you'll be aware of poor patterns susceptible to attack.You can change them if you're culpable of the same mistake or keep away from them in the future.You could even raise awareness by enlightening your friends on proper practice.Those in places especially like the **United States** are lucky because of services like the Have I Been Pwned site(haveibeenpwned) which let's users see if their accounts and personal information have been revealed in previous data breaches.

VII)Only visit sites you know and that use secure HTTP(HTTPS) and other secure network protocols.Change your password in case a site you had visited gets breached.

5]Networks and their Security Flaws



WEP

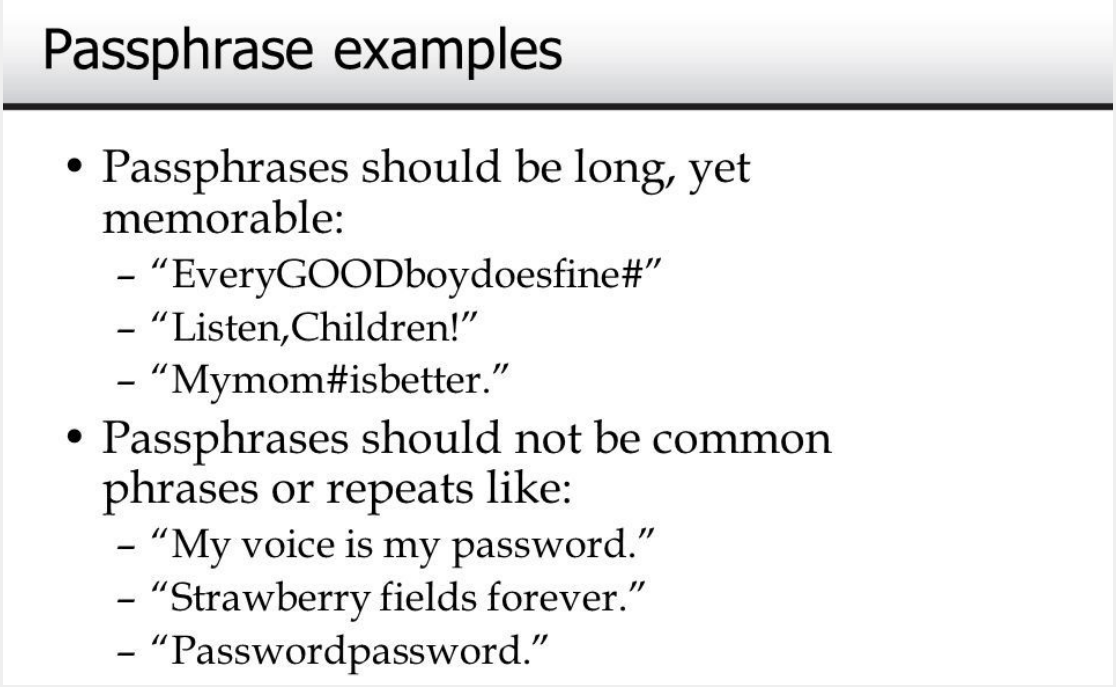


--> For those of us who love free Wi-Fi

Wired Equivalent Policy(WEP) is an old IEEE802.11 Standard from way back in 1999.WEP had an original encryption protocol for wireless networks and uses wireless routers to transmit data with devices such as computers.The basic principle behind Networking is that resources and information are shared in the form of data packets;to make transmission easier.The packets follow a certain order and then follows the **OSI**(Open System Interconnection) model that consists of 7 layers.The OSI model links up the devices connected to the network for the purposes of Networking we have stated.Networking is a form of traffic (**with data packets moving across it**).Packet sniffers and analyzers(e.g **Aircrack-ng**,**Wireshark**) can be used

to view the data packets and thus intercept the data.WEP was initially designed to provide the same level of security as Wired networks.WEP however is difficult to configure and is easily broken,an issue that prompted a search for other alternatives like WPA/WPA2.

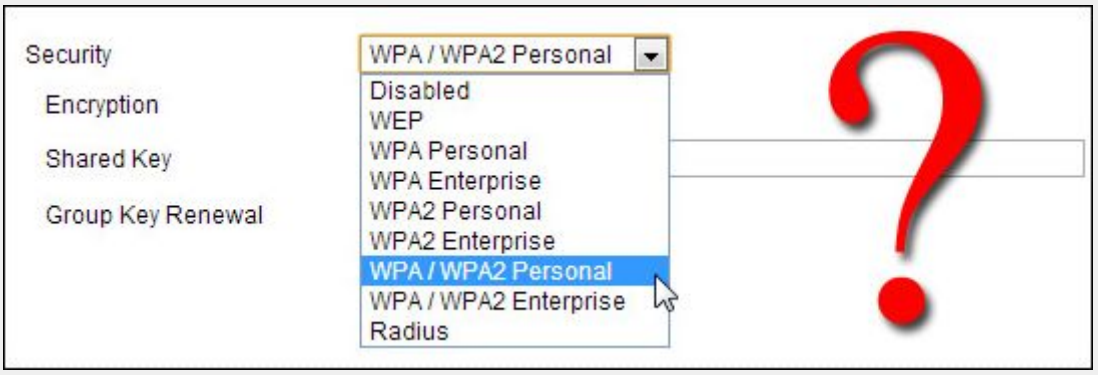
Passphrase - A password which is purely formed from words.



The **IEEE** and **other industrial players** came up with the WPA/WPA2 protocol and its other generations to address the shortcomings of the WEP. The industry largely tired by WEP's numerous flaws,literally forced people to change to WPA/WPA2 encryption (**this by limiting the speed between computer and routers to 54mbps on wireless routers**).

It is indeed cool to set up a home Wi-Fi,but to enjoy this feature you have to take care of the WiFi flaws which could give your password easily and giving access to attackers to get into the network and carry out successful exploits.The first step is to come up with a password, then when the machine requires you to select the type of encryption standard; you should choose WPA2.Don't select Default because most machines default to WEP/WPA(which are not secure networks).During the configuration process,the router also asks you whether you want to hide the **SSID**:"Hide the SSID? ".You should not select yes because if you do,your devices will be forced to actively scan for the network you're trying to hide- They will ultimately connect but this shall be the new normal each and every time (**your devices will always be actively scanning for networks**).This makes the devices susceptible to connecting to other 'unsafe' WiFi networks

WPA/WPA 2



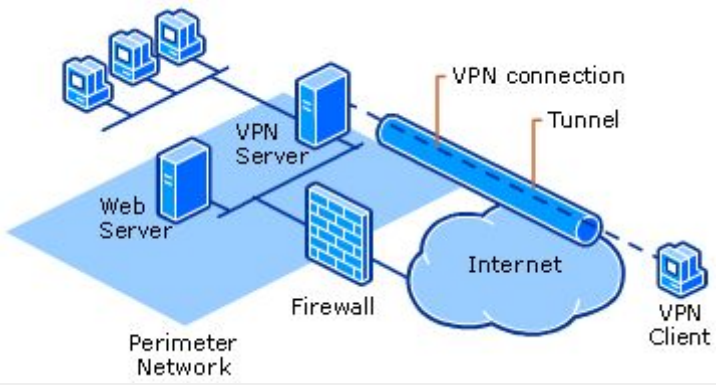
Wireless Point Access was designed to be a temporal/interim enhancement over WEP whilst work on the 801.11i Wireless Security was on going.WPA2(The second generation of WPA) is an implementation of the IEEE 802.11i wireless standard.It implements a PreShared Key (PSK) or WPA Personal alongside an encryption known as TKIP(Temporary Key Integrity Protocol)- in which there is key mixing with a re-keying system whilst also providing a message integrity WEP; all of which are fundamental in avoiding the problems of WEP.The industry has been largely successful in phasing out the use of WEP but there are reports of WEP still being in use as late as 2010.If anyone still uses WEP technology;it is not a matter open for debate and they should move to WPA/WPA2 **ASAP**!.

Using a long enough random password (such as 14 random letters or a passphrase (of 5 randomly chosen words) makes WPA virtually uncrackable.If a weak password, such as a real word,dictionary word or a character string used,WPA/WPA 2 is still vulnerable and can be cracked.Weak passphrases can be broken using off-line dictionary attacks;**Aircrack-ng**,**Auditor Security Collection** and **Airsnort** will crack a weak passphrase in minimal time.The WPA,if used with good passphrases or a 64-character hexadecimal user key is still secure.WPA 2 was finalized in 2004 and based on the 802.11i Wireless Standard.WPA2 is better than WPA since it uses an Advanced Encryption Standard(**AES**) for Encryption,AES Technology is so top notch and reliable that the **US** government uses it to encrypt information that it regards as '**top secret**' or '**classified**'.WPA2 however has a security flaw,nicknamed Hole 196(from page 196 of the IEEE 802.11i specification in which the vulnerability is discussed).The vulnerability makes use of the WPA2 Group Temporal Key(GTK);which is a shared key among users of the same BBSID(The MAC Address of an access point) to launch attacks on users of the same BBSID.However,in order to exploit this vulnerability successfully,the GTK must be known by the attacker.

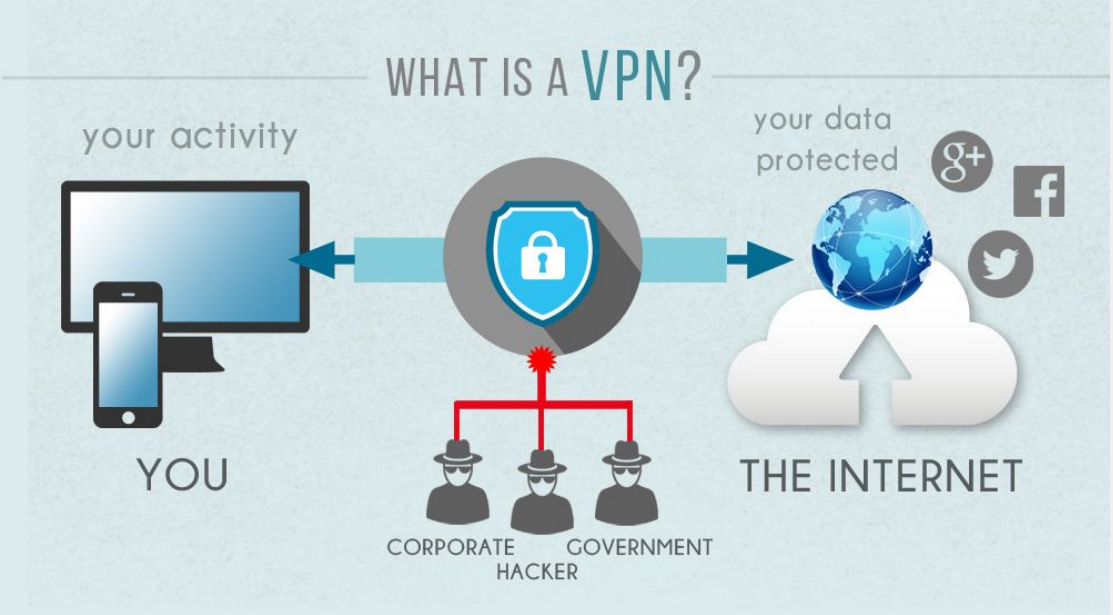
WEP VS WPA VS WPA2

	WEP	WPA	WPA2
ENCRYPTION	RC4	RC4	AES
KEY ROTATION	NONE	Dynamic Session Keys	Dynamic Session Keys
KEY DISTRIBUTION	Manually typed into each device	Automatic distribution available	Automatic distribution available
AUTHENTICATION	Uses WEP key as Authentication	Can use 802.1x & EAP	Can use 802.1x & EAP

VPNs(Virtual Private Networks)



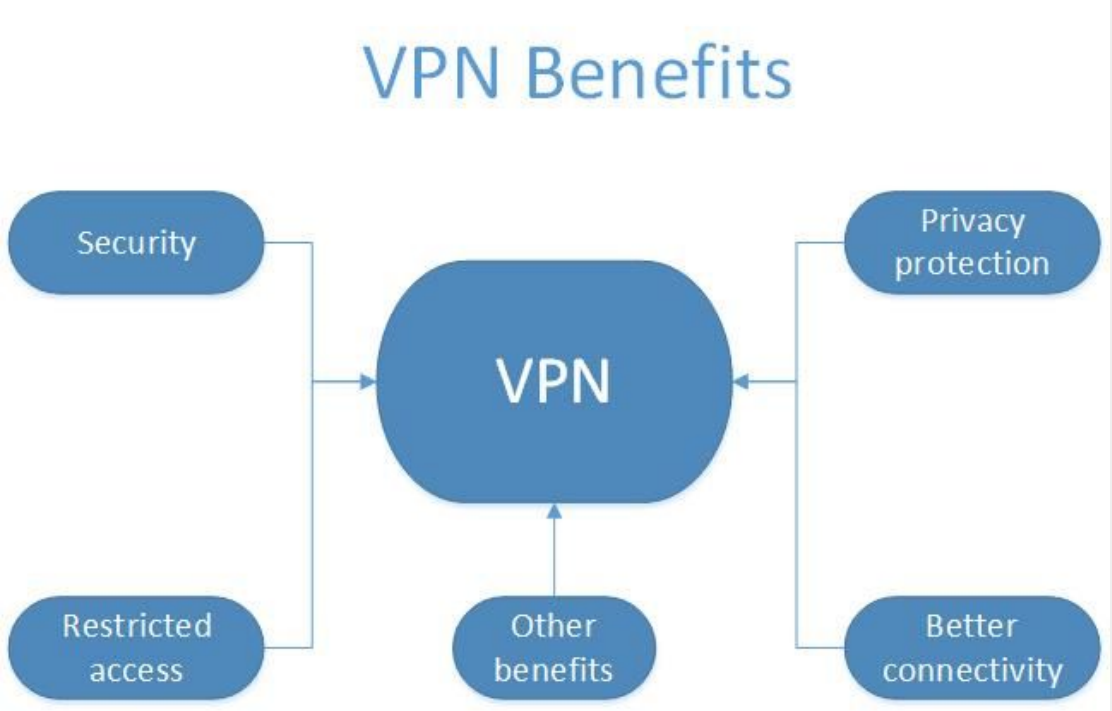
A virtual private network is an extension of a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network which creates a secure,encrypted connection between your computer and a server operated by the VPN Service-with this connection being thought of as a tunnel.Individual internet users may secure their wireless transactions with a VPN,to circumvent geographical transactions and censorship,or to connect to proxy servers for the purpose of protecting personal identity and location because using VPNs should completely hide your IP address.VPN's Virtual connections are routed through the Internet from the private network to a remote site.



Proxy server-A virtual server which is used to access the a network or the Internet whilst giving some degree of anonymity(you can still be tracked down!) of **identity** and **location**.It gives you another IP address and thus you don't use your devices' IP address.

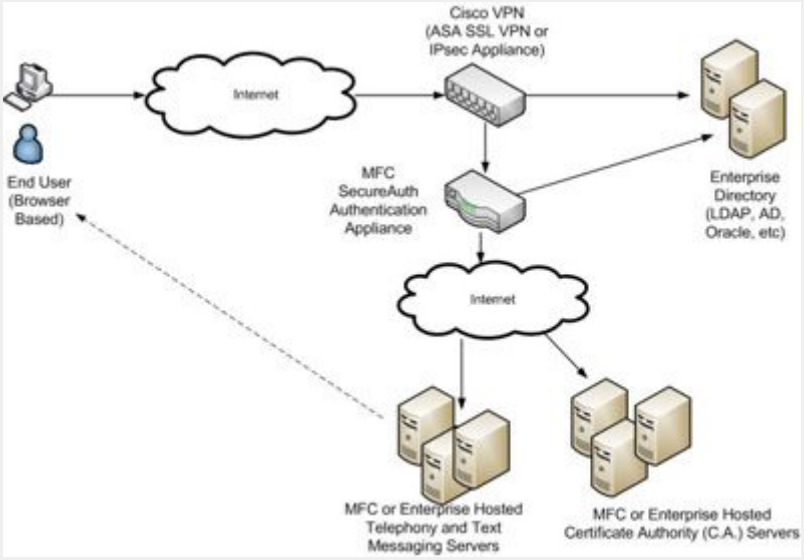
VPNs cannot make online connections completely anonymous,but they can usually increase privacy and security.To prevent disclosure of private information,VPNs typically allow only authenticated remote access using tunneling protocols and encryption techniques.The VPN Security model provides:

I. **Sender authentication to prevent unauthorized users from accessing the VPN.**
II. **Confidentiality such that even if the network traffic is sniffed at the packet level,an attacker would only see encrypted data.**
III. **Message integrity to detect any instances of tampering with transmitted messages.**

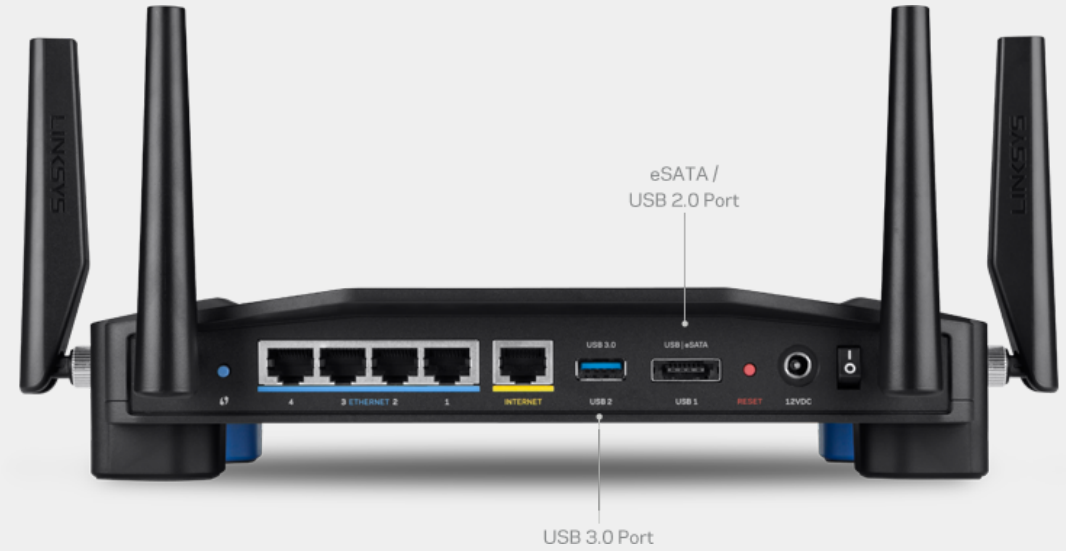


VPN Authentication

We have already seen that VPNs establish a connection which can be viewed as a tunnel.Tunnel endpoints must be authenticated before secure VPN tunnels can be established.User-created remote-access VPNs may use Passwords,Two-factor authentication,Biometrics or other Cryptographic methods.Network-to-Network tunnels often use passwords or digital certificates.They permanently store the key to allow the tunnel to **establish** connection automatically,without intervention from the administrator.

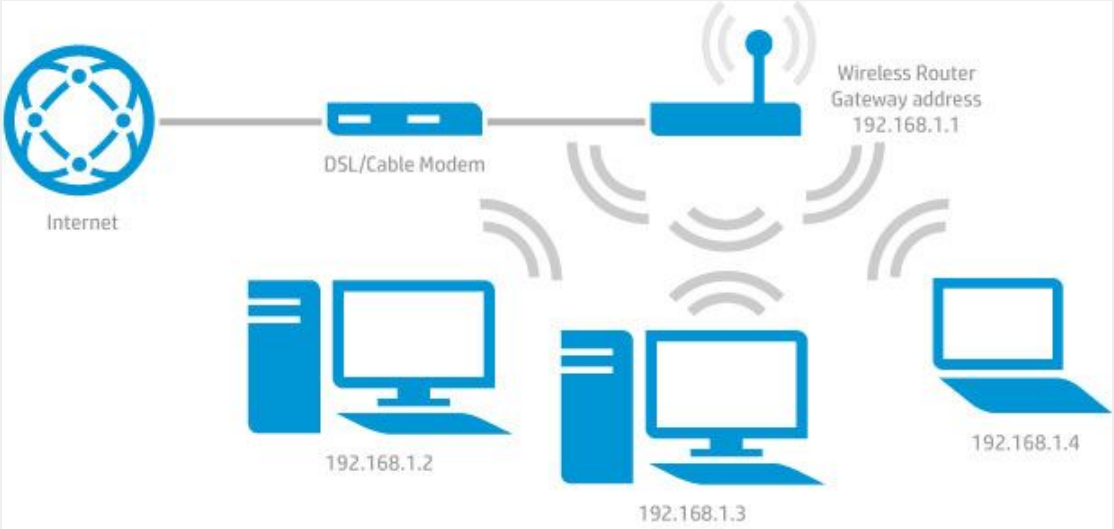


Routers

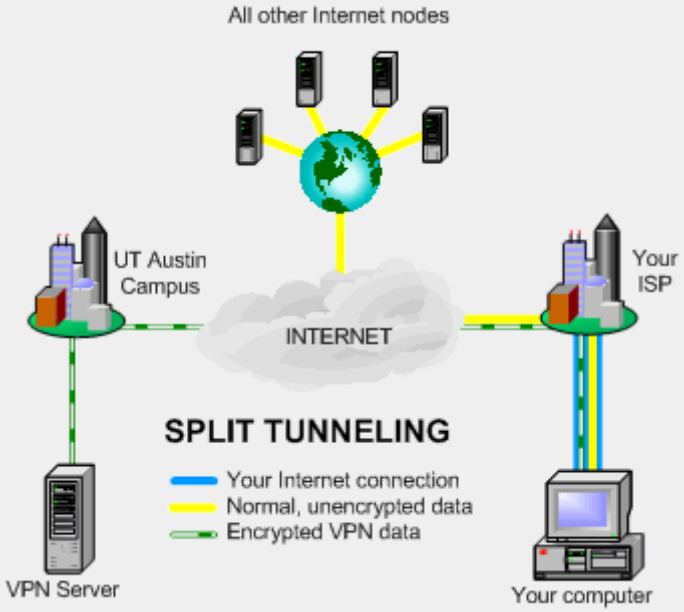


Routers as we know them,are basically devices that are used to wirelessly transmit data packets to devices and establish network connections.Routers are very common **nowadays**.Router manufacturers such as **Asus,Cisco,DrayTek,Netgear,Yamaha** and **Linksys** provide routers with built-in VPN clients.Most router implementations support a software-defined tunnel interface,customer-provisioned VPNs often are simply defined tunnels running conventional routing protocols.Due to the popularity of VPNs,VPN connectivity on routers is being set up for additional security and encryption of data transmission by using various cryptographic techniques.However,setting up VPN Services on a router requires a deep knowledge of network security and careful installation.Minor misconfiguration of VPN connections can leave the network vulnerable - and performance largely varies depending on the ISP(Internet Service Provider).If a VPN support is set up on a router and the VPN service being established allows any networked device to have access to the entire network - in which all devices look like local devices with local addresses with supported devices not being restricted to those capable of running a VPN Client.



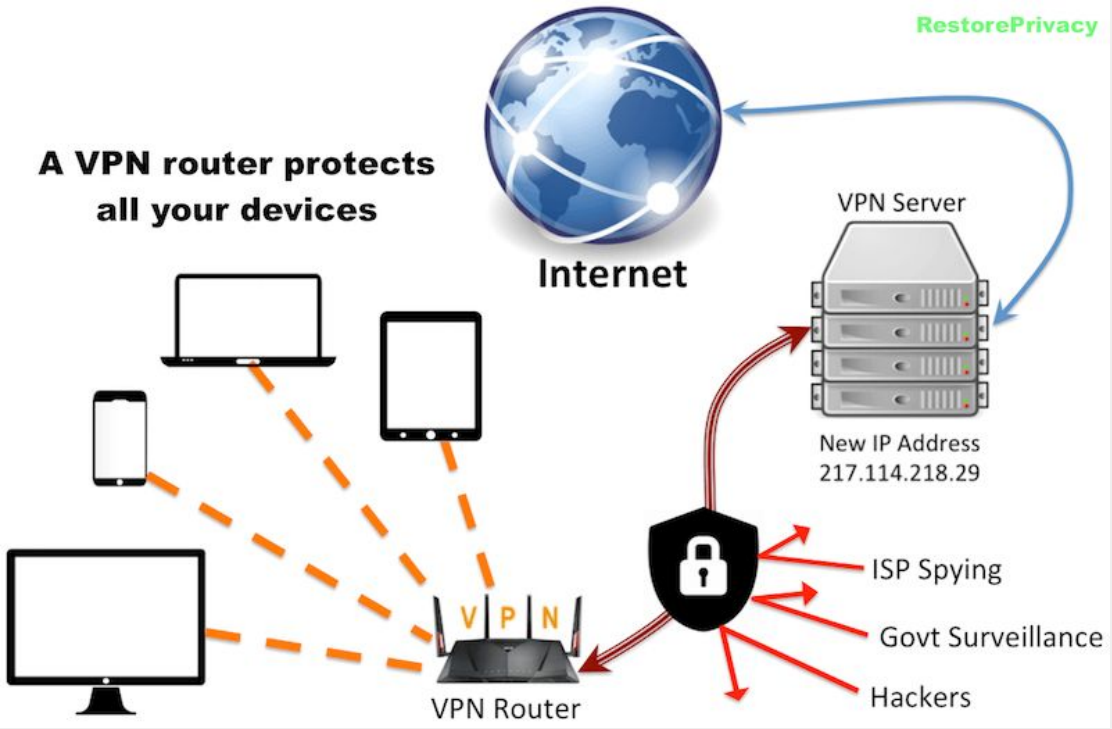


Unencrypted Tunnels



Some virtual networks use the VPN tunneling protocols without encryption for protecting the privacy of data in the network.Such an encrypted network is not as secure or trusted and is therefore not a recommended practice.Trusted VPNs do not use cryptographic tunneling,instead relying on the security of a single ISP provider's network to protect the traffic.From the Security perspective;Unless the trusted delivery network runs among physical secure sites only,both the trusted and secure models need an authentication mechanism for users to gain access to the VPN.

VPNs In Private Networks



-->Data roaming....

Mobile VPNs are used by people requiring reliable connectivity i.e Roaming seamlessly across networks and in and out of wireless coverage areas without losing application sessions or dropping the secure VPN session.These mobile VPNs are used in settings where an endpoint of the VPN is not fixed to a single IP address,but instead roams across various networks such as data networks from cellular carriers or between multiple Wi-Fi access points.A conventional VPN cannot withstand events such as roaming because the network tunnel will be disrupted,thus causing applications to disconnect,timeout or fail,even cause the computing device itself to crash.Instead of logically tying the endpoint of the network tunnel to the physical IP address,each tunnel is bound to a permanently associated IP address, each tunnel is bound to a permanently associated IP address at the device.Mobile VPN software handles the necessary network authentication,whilst **maintaining** the network sessions in a manner transparent to the user.

Limitations Of VPNs

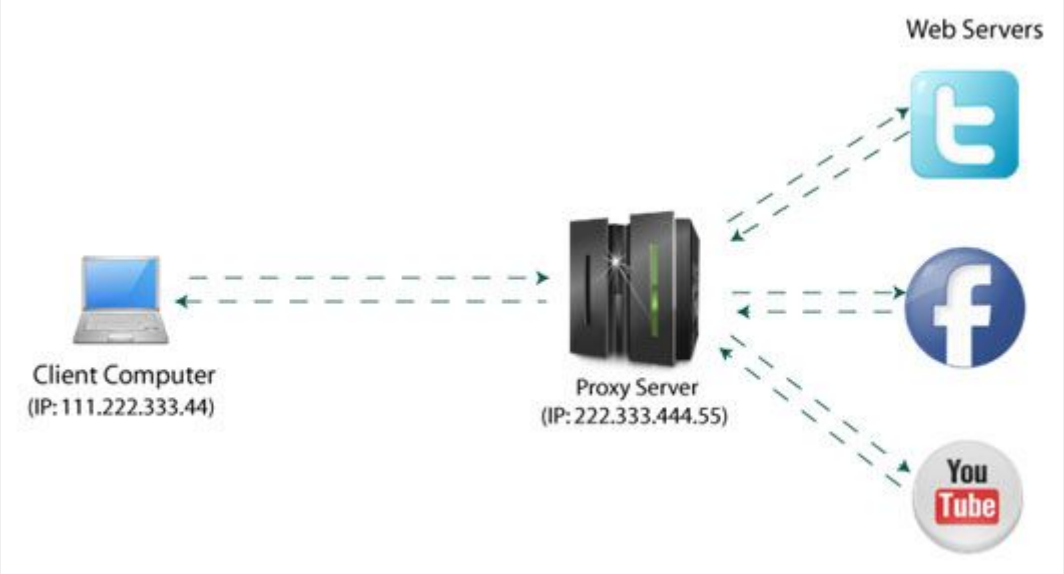
- VPNs operate at OSI layer 3 through 7 in contrast to 802.11security mechanisms that operate at layer 2.
- VPNs over wireless is not always the best choice because of the limitations of VPNs can place on wireless mobility and scalability.

Traditional or Conventional VPNs are point-to-point,and therefore do not tend to support or connect broadcast domains.This limitation results to the Communication,Software and Networking which are based on Layer 2(**of the OSI Model**) such as **NetBIOS** used on Windows Networking,may not be fully supported or work exactly as they would on a real LAN.To this effect,variants of the VPN such as the Virtual Private LAN Service (**VPLS**) and layer 2 tunneling protocols have being designed to overcome this limitation.

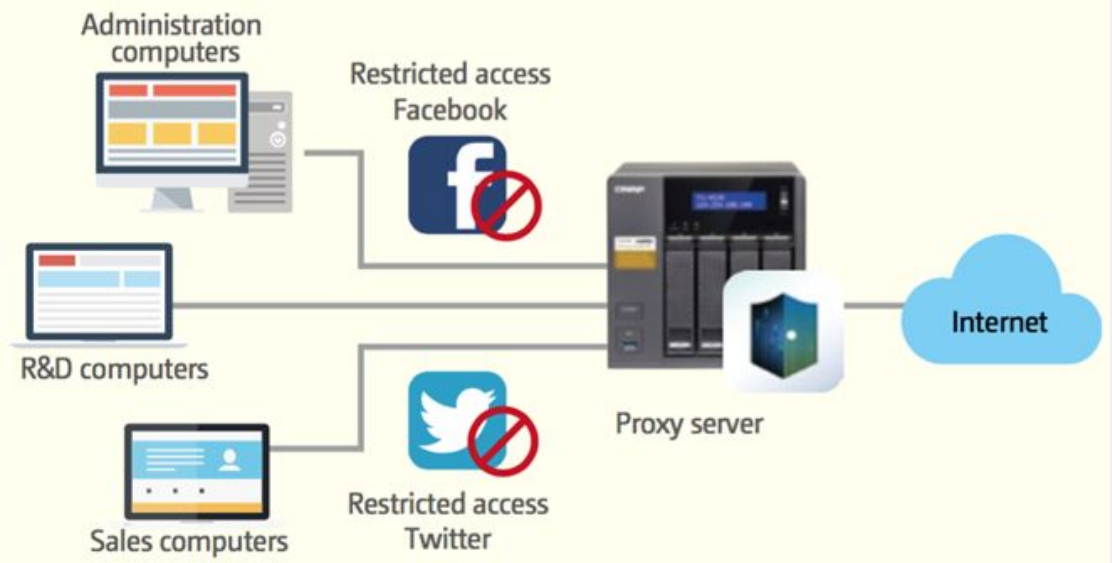
VPN Disadvantages

- Management
- Availability and performance
- Interoperability
- Additional protocols
- Performance impact
- Expense

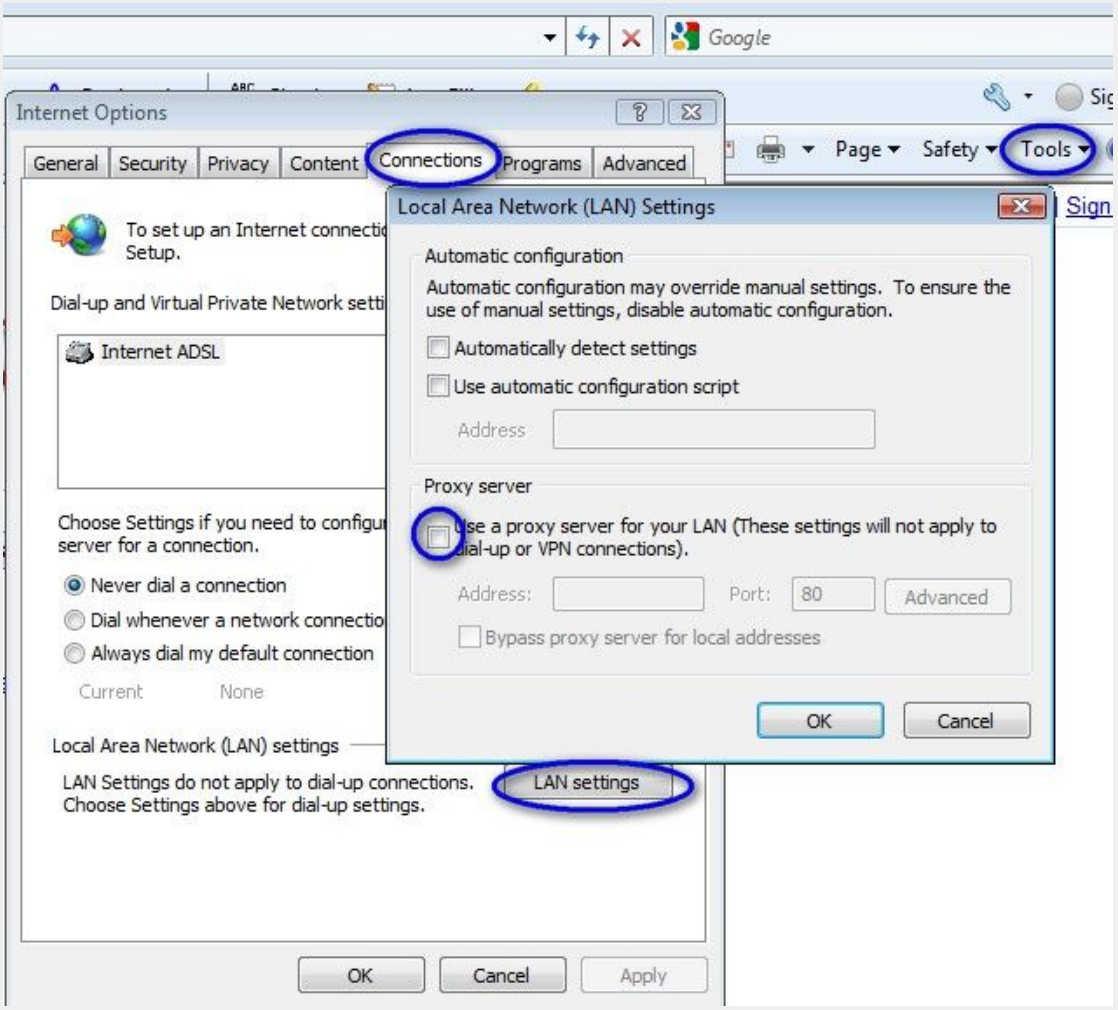
Proxy Servers



The general meaning of a proxy is anybody or an agent/substitute acting in place of another.Proxy Servers simply act as an intermediate between your machine and the actual server that you are accessing.They are mostly used to maintain anonymity and therefore can be used to bypass some firewall restrictions.The actual web server doesn't come to know about you because the proxy server is dealing with the webserver on your behalf.Proxies are ideal for use to visit any website without your Internet Service Provider or anyone else finding out.For Example,In many **companies** and **schools**- firewalls are configured to block people who try to use the Internet for purposes such as accessing social networks(**especially Facebook**)which would be seen as promoting casualness.The proxy server will bring to you the Facebook webpage and serve you,leaving the firewall to assume that you are dealing with a server other than Facebook and gives you the greenlight to make a connection- you will have successfully bypassed the firewall.There are various types of proxy servers some of which offer anonymity,others still make the original IP address available through the http headers(i.e **Anonymous Proxy,Distorting Proxy,High Anonymity Proxy and Transparent Proxy**).It is wise to know the type of proxy server;its features and risks first before going ahead to use it.



Configuring Proxy Servers

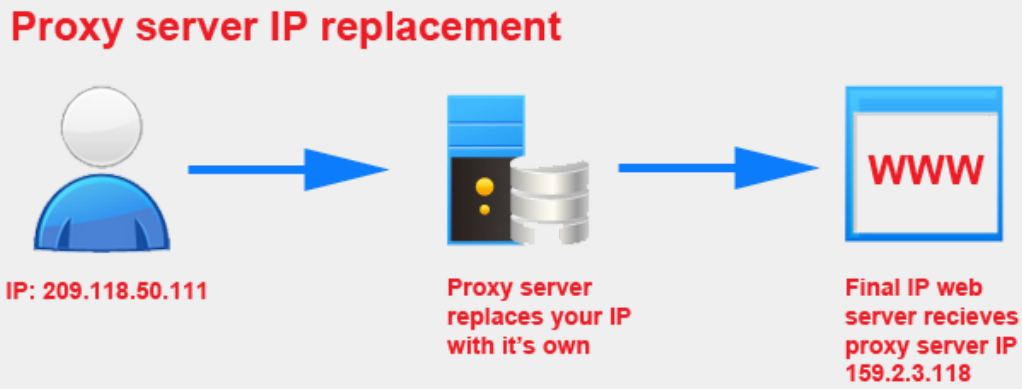


1)The proxy server can be set up in web browser
2)Log onto [whatismyip.com](whatismyip.com) and write your current IP.
Go to google and search for 'proxy servers list'.You will get a list of many sited with proxy servers(the IP address) and their port numbers i.e IP:Port plus the country of location. Do this bearing in mind that it is illegal to use proxy servers without the permission of the owner;be it in some States in the United States and other Countries.
3)Copy the IP and port number.
4)Using the proxy on various browsers:
(i)Mozilla FireFox Browser> Go to Options> Advanced tab> Network> Settings> Check the option 'Manual Proxy Configuration'> Fill IP and Port No and you're good to go.

(ii)Safari 2.0.3> Under the Safari tab> Advanced> Next to " proxies" Click on "change settings" (which will open the system network preferences)> Ensure that the correct connection method is in the "show" window(e.g built-in Ethernet)> Check the box next to HTTP> Enter the proxy server's IP address in the first box and the proxy's port in the box after the ":" > Select Apply Now.

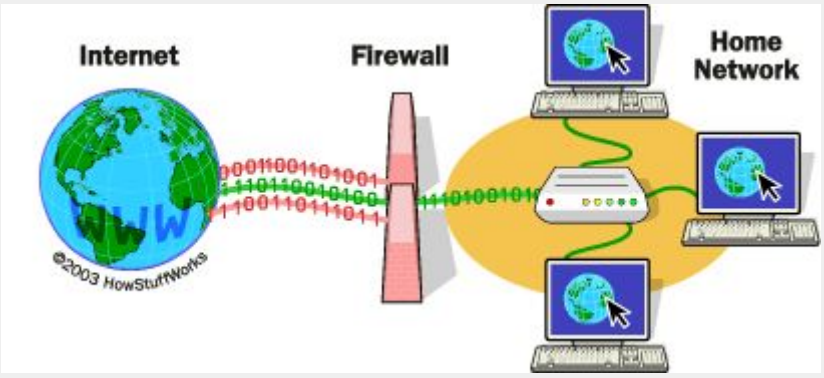
(iii)Netscape 8.1> Go to Tools> Select Options> General- that is connection settings> Check Manual proxy configuration> Enter the proxy server's IP address in the HTTP proxy field and the proxy's port in the port field> Click OK.
(iv)Opera 8.5> Go to Tools> Select Preferences>Advanced>Proxy Server's> Check the box next to HTTP> Enter the proxy server's IP address in the first box and the proxy's port in the box after "port"> Click OK.

As you can tell,most of the configuration process is more or less the same irregardless of whatever browser you are using.The basic thing is to first have the IP and Port Number you want to use.
5)Check out whatismyip.com again,to confirm if your IP has successfully changed.



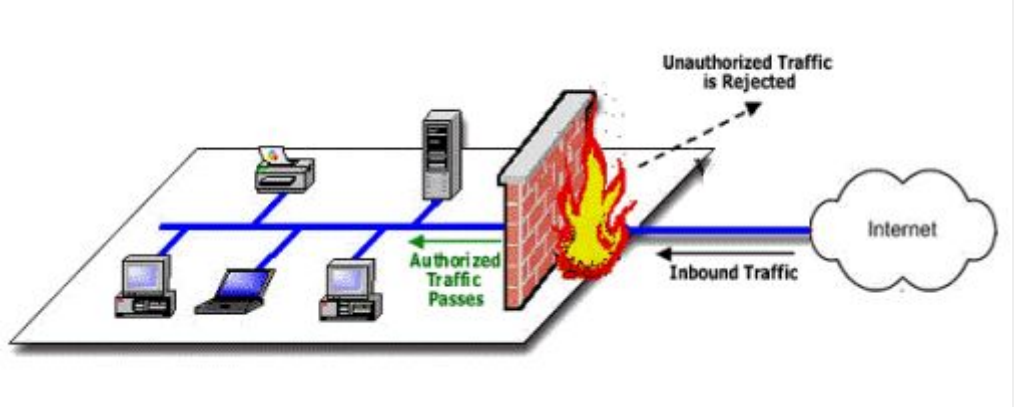
It is also possible to use Softwares and Applications.IP hiding softwares are easy to use and freely available on the internet.Such applications and programs keep changing your IP address automatically after a particular interval of time e.g **Ultrasoft**.Websites also provide proxy servers services, which are free and can be used to visit other websites e.g hidemypass.com

Setting Up Firewalls



A firewall is a way of filtering network data between a host on a network and another network,such as the Internet,and can be implemented as software running on the machine,hooking into the network stack(**or,in the case of**

most UNIX-based as systems such as Linux,built into the OS kernel)to provide real time filtering and blocking.**Windows** and **Mac** based PCs come with built-in firewalls, but there also exists third party software and their features and usability by far exceed these native firewall programs.If properly configured,firewalls can shield access to internal network services, and block certain kinds of attacks through packet filtering.Only traffic that matches defined rules is allowed to pass.They often include detailed logging, and may include intrusion detection and prevention feature.Firewalls can be Hardware or Software based.Another implementation is the "physical firewall",which consists of a separate machine filtering network traffic.They are most common amongst machines that are permanently connected to the Internet.A firewall will help protect your computer from hackers who might try to gain access to crash it,delete information or even steal passwords or other sensitive information.Software firewalls are widely recommended for single computers.The software is prepackaged on some Operating System or can be purchased for individual computers.For multiple networked computers,hardware routers typically provide firewall protection.



If you use a lot of Internet-connect programs or mostly visit unscrupulous sites,a firewall could spare you from the malware headache and its accompanying economic pinch.Some third-party firewall programs include:

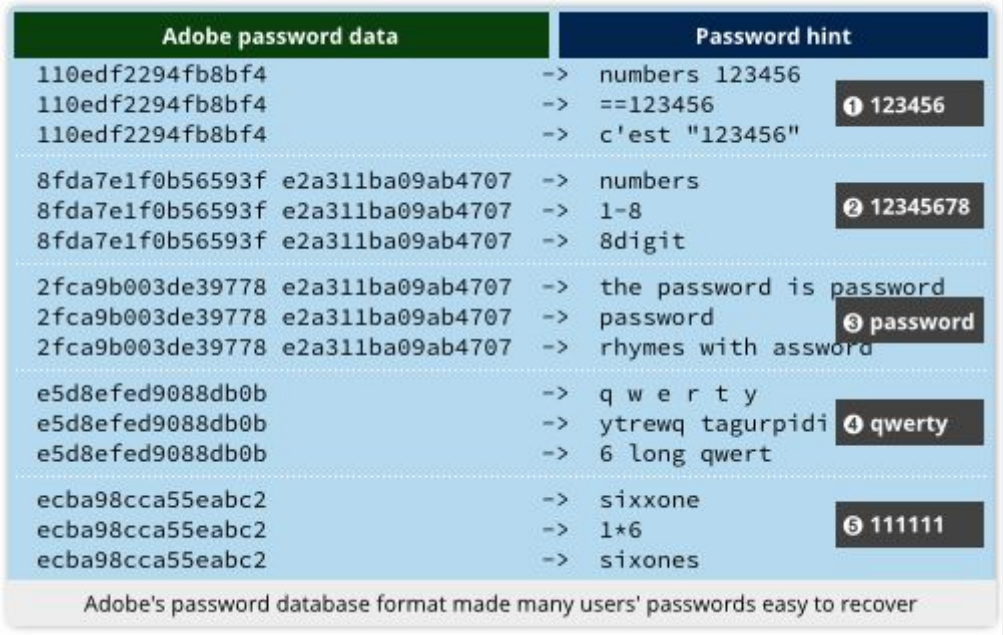
(I)**Tinywall-** Only 1 Mb in size and runs as a standalone option.A whitelist option, port and domain blacklists, a way to restrict applications to LAN only access,IPv6 support,Password lock on settings are some of it's features.
On its downside(defects of free software),it doesn't give pop-ups and notifications on the real time security situation instead comfortably running in the background.

(II)**AntiNetcut3-** This is an app which is specifically designed to safeguard your PC when your are on insecure networks- especially public Wi-Fi.It is also very good at protecting against Deliberately cut connections,Protecting against ARP(**Address Resolution Protocol**) spoofing amongst other forms of connection manipulation.The English language though,has some translation issues and the interface is plainly basic you would pass it for an amateurish creation,but its work is very good.

(III)Comodo Free Firewall
This app is one of a kind.Unlike most other firewall programs, the app draws a cloud-based directory of more than two million "safe" apps.This enables the app to alert you if something that's not on the safe list tries to access your machine.Unlike Tinywallfirewall,It gives pop-ups and notifications to keep you updated with your real-time security situation.There is also a premium version with the company's professional anti-virus suite,more firewall options and around the clock support. So sure are they of their anti-virus program's efficiency that they offer a '$500 Virus Free Guarantee'.The premium version costs $40 per year.Others are **Peerblock**,**Littlesnitch**(for **Mac** only),**PrivateEye**(**Mac** only) and **Zonearm**($40 per year).

6]Problems With the Web and Securing it

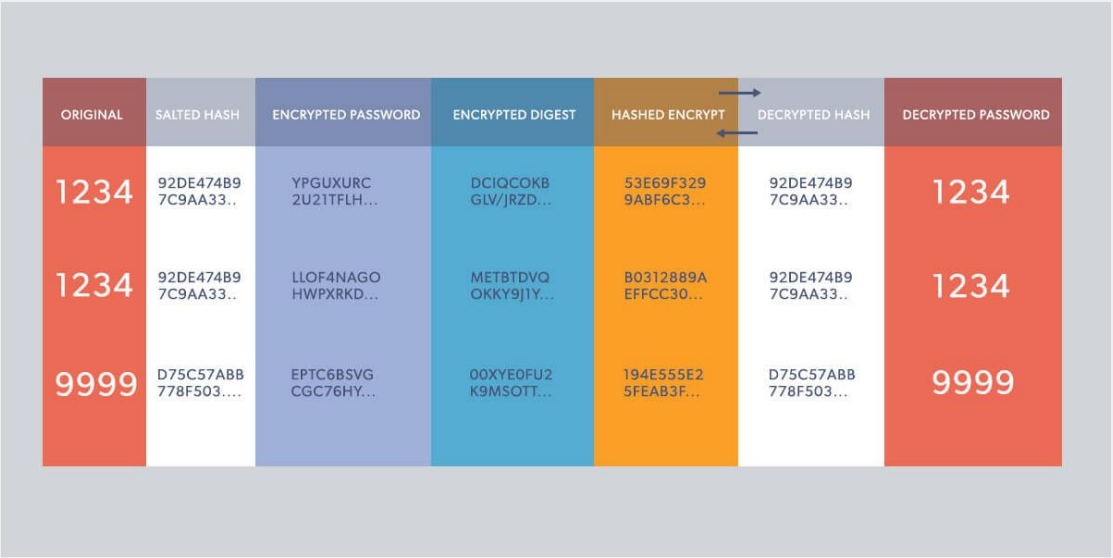
Storage of Passwords On the Web



Adobe's password database format made many users' passwords easy to recover

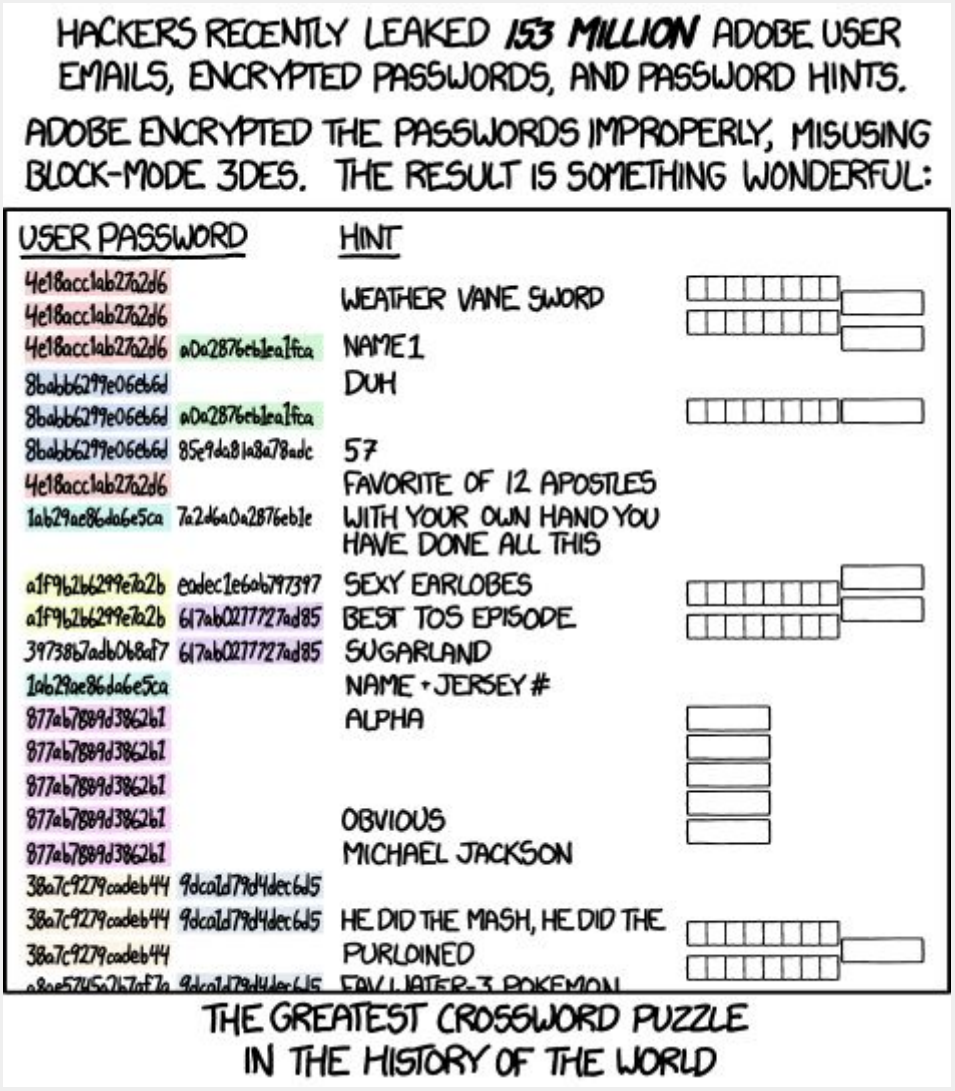
When you sign-up for a website, your data is usually stored in a database on servers.If a password is stored as plaintext,an attacker who gains access to the server will obtain these passwords.So,when hackers breach the server, they can't steal any passwords – only hashes.We earlier saw that hackers can identity hashes by using the same hashing algorithm to generate hashes,compare them and when the two hashes match then the password is cracked.(**The salt must be saved for each user and is usually stored**

beside the username and password hash,so the information is available during each user login.Salt is rarely kept apart from the hash.Even when known,its virtue lies in its uniqueness,which defeats pre-computation of results).

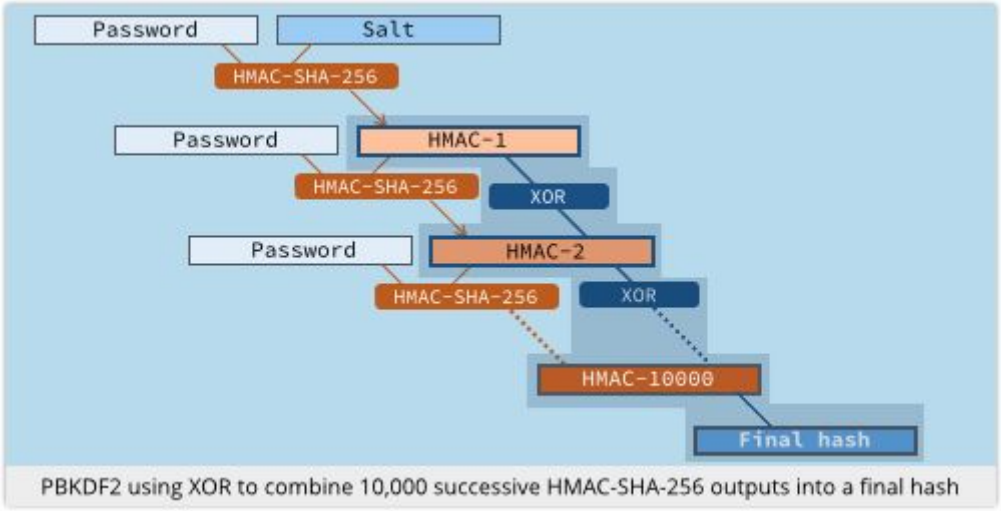


Solution:Online Services should always make sure that passwords are never stored as plaintext but are properly hashed and salted using proper algorithms.

Poor Encryption,Hashing and Salting Techniques



Websites should be very careful when using password-hashing functions.Not all encrypting software can be used for hashing,as we have already seen.Proper research and a well-audited proven function such as **Bycrypt** and **Scrypt** should be used.There have been many data breaches in recent years,with some irregardless of the hashing function used but the first step to protecting the website's users.Algorithms such as **SHA-1**,**MD5** and **SHA3** are out of the question when it comes to considering hashing functions.In October 2016,an online dating company **Adult Friend Finder** was breached and over 412.2 Million user accounts were compromised.As it is always the case a lot of user data such as Names,Email Addresses and Passwords were stolen by the hackers.All this data had been collected for two decades.Majority of the passwords were protected using the same poor and weak hashing functions I have talked about- the SHA-1 Hashing Algorithm.



PBKDF2 using XOR to combine 10,000 successive HMAC-SHA-256 outputs into a final hash

There are challenges when it comes to implementing proper Salting and this is largely because many websites have millions of users.Using the same salt for each and every single user will leave the website vulnerable to a rainbow table attack.The attackers will generate a custom rainbow table for this site and attach your salt to it.The solution to this is to use random salts.The attacker can therefore not try to obtain all the passwords from the database.This is virtually impossible to achieve due to the large storage and memory required plus also considering the time factor.There will be no challenges to the server,as it will simply store the username and password hash along with the randomly generated salt and it will use it again when the user enters the password for Comparison.The attackers remaining option would be to target a specific user,by trying to generate a rainbow table specifically for that salt,this would take a long time and if the user has a strong password there would be too many character combinations that could be contained in the password.

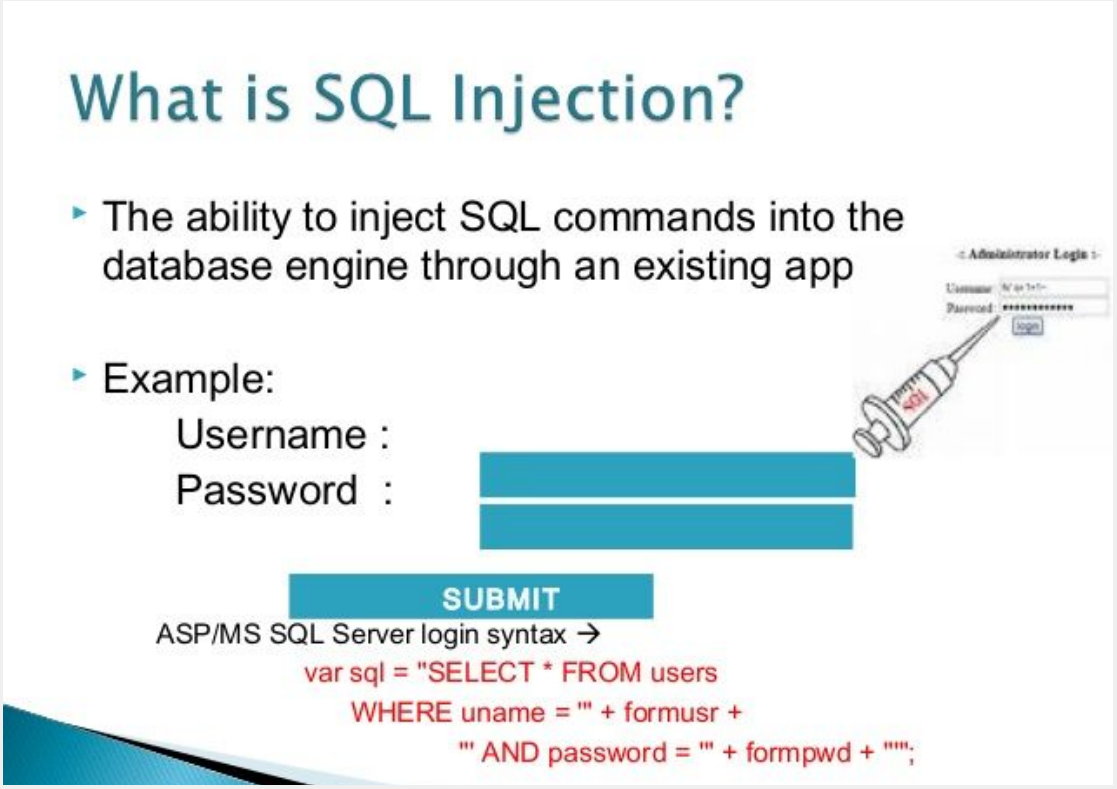
Website Hacks

Injection Attacks



This is the most popular method of getting access to web servers.It will usually

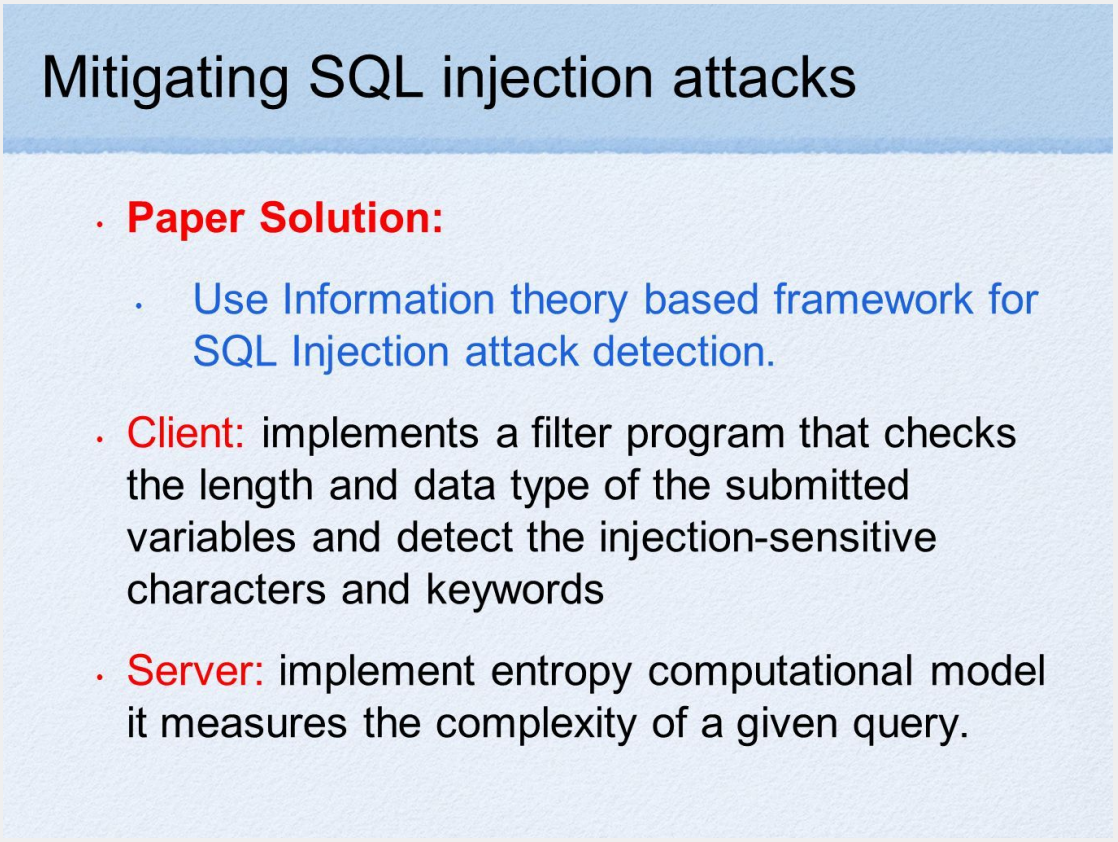
occur when there are flaws in the **SQL** Database,Libraries or even the Operating System itself.SQL is **Structured Query Language**,a query language used for accessing and modifying information in a database.Injection attacks is the exploitation of a computer bug that has been caused by processing invalid data.The attacker will inject the code into a vulnerable program to change the mode of execution.If successful,the code injection results in faster computer worms propagation.The flaws or bugs in computer programs that are exploited by code injection come about when an application send untrusted data to an interpreter.Scanners and Fizzers can catch this flaws because injection flaws tend to be easier to discover when examining source code than through testing.Other injections are XSS Injection and LDAP injections in the web application among others.If password checking isn't rigorous enough,hackers easily bypass the system and get confidential user data.SQL uses simple queries to obtain information requested by users which makes it a piece of cake for the hackers!Source code could also be injected to change the website code as in the case of **Adult Friend Finder** in 2016,where through an injection vulnerability one could access the site's source code.Password Cracking tools such as **Wfuzz** can be used to achieve this.



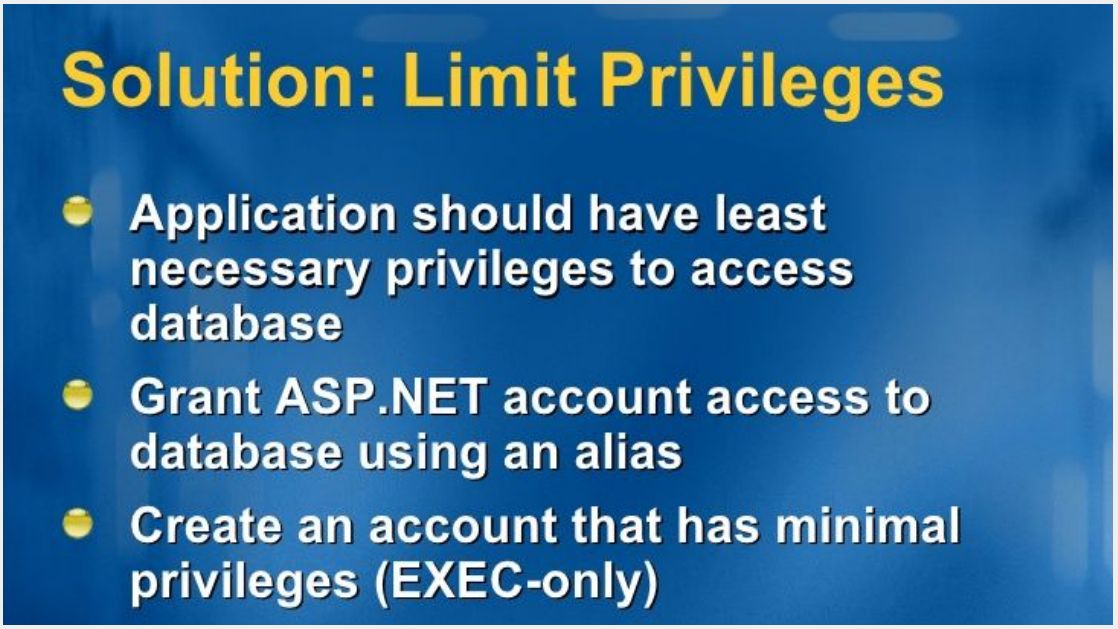
Another way is where the attacker's gain "root" privilege which means unlimited or admin access to the server,through privilege escalation and exploiting shell injection vulnerabilities in **UNIX** or **Local Systems** and **Windows**.The most prominent example of this kind of attack involved **JP Morgan Chase**(the largest bank in the **US**) back in 2014,whereby personal details(names,addresses,phone numbers and email addresses) of 76 Million households and 7 million small businesses were compromised.The attackers

had gained "root" privileges.Admin permissions that are not restrictive enough and allow anyone to edit the database file on the server or misuse of passwords by website hosting companies- such that the database password is the same one for accessing network protocols like FTP and SSH.Attackers with access to configuration files from website support platforms and plugins like **Joomla**,**Drupal** and **WordPress** will therefore be able to extract the login password for the user and use it to access the server.

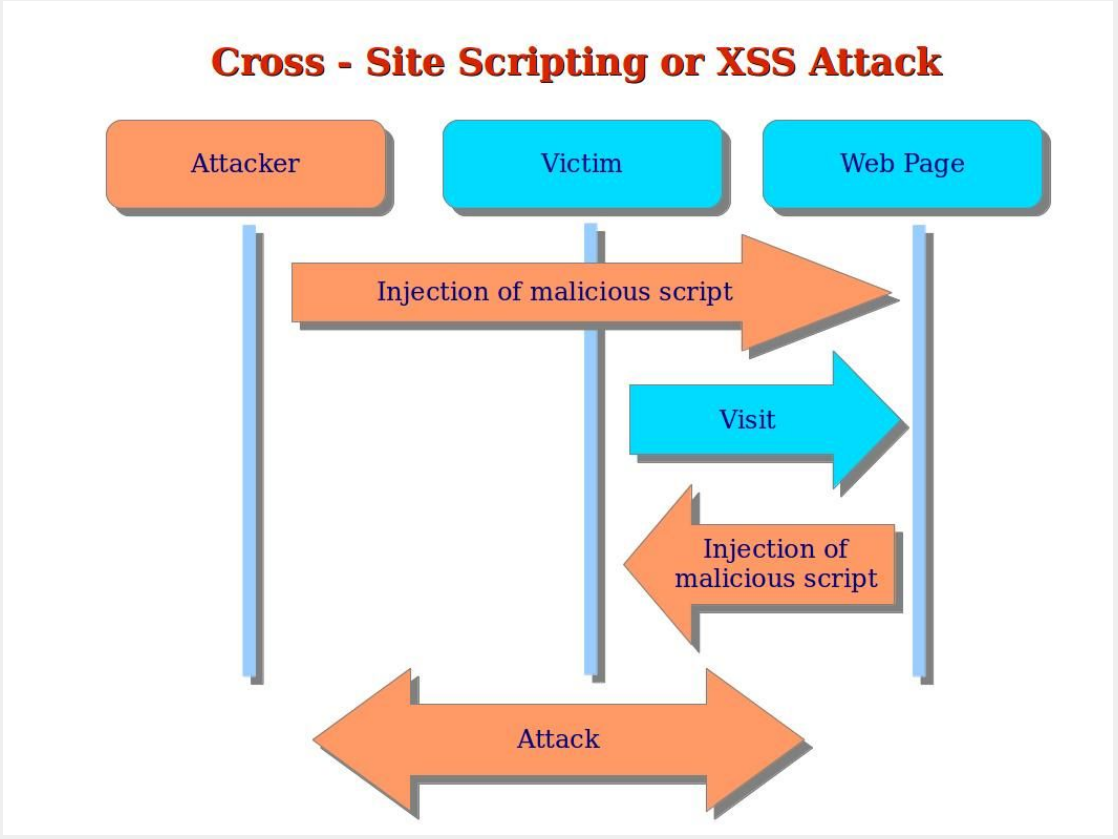
Solution:



1)*Whitelist Input validation- Allowing only known proper values to combat code injection vulnerabilities.*
2)*NX bit- Where all user data is stored in a special memory section that is non-executable.The processor refuses to execute anything from this part because it has been made to understand that no code exists in that part of the memory.*
3)*Hiring of Professional Security Support to help with proper management of the Web Server.*
4)*Be careful about the permissions you set on the web server.*

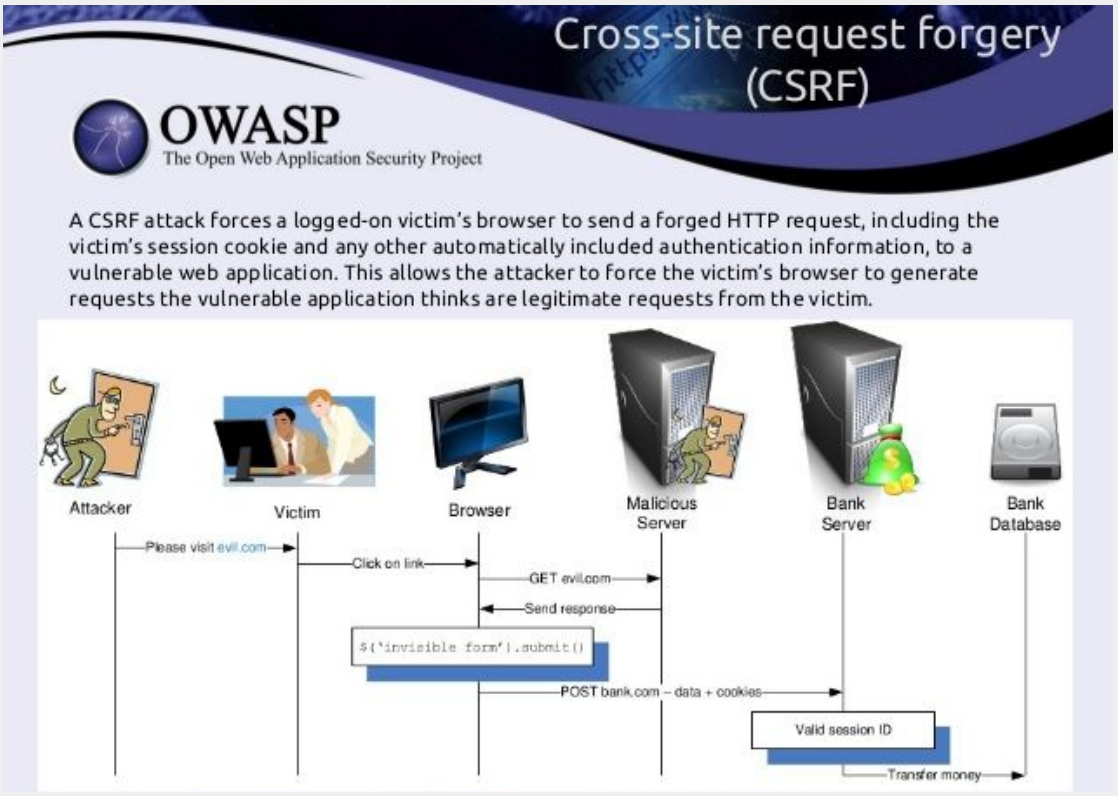


(1)*Cross Site Attacks*

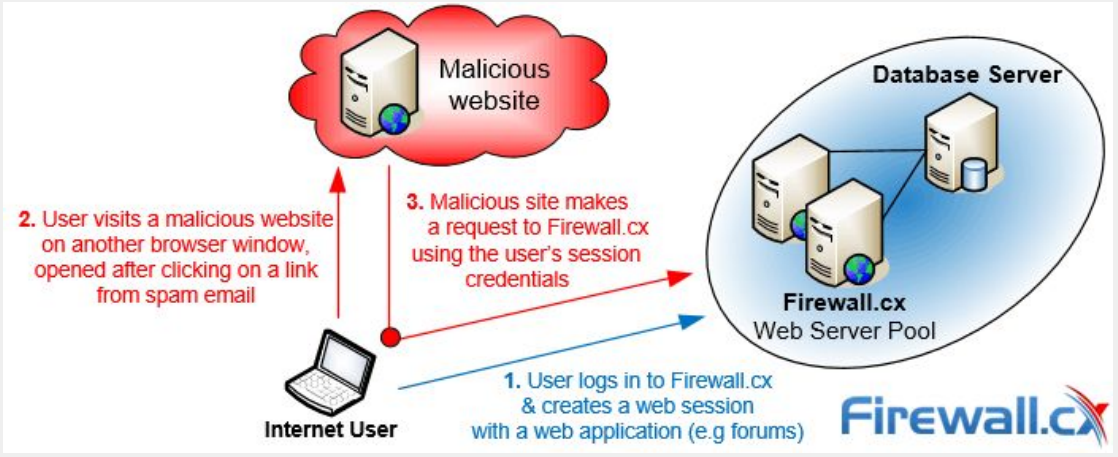


There are two types:

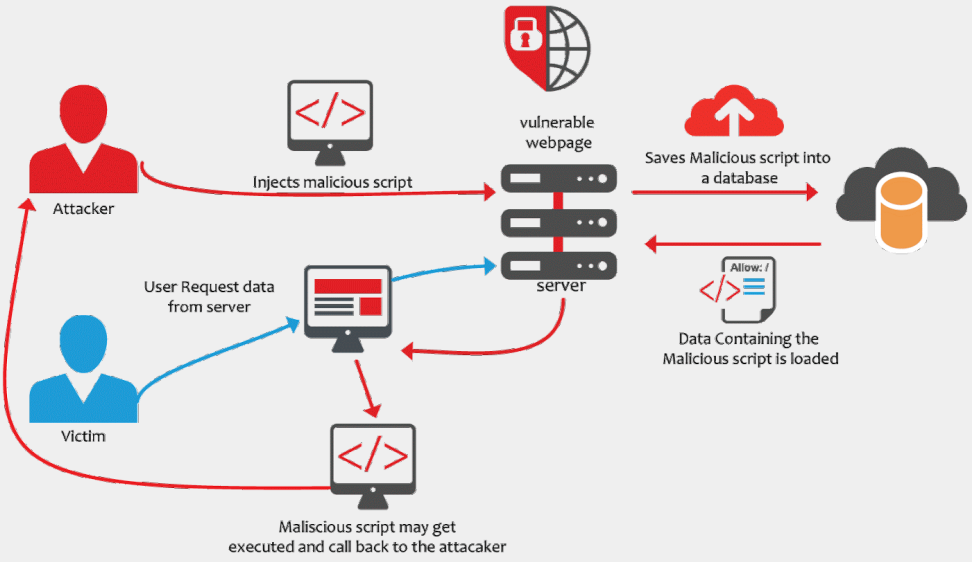
(a)Cross Site Request Forgery



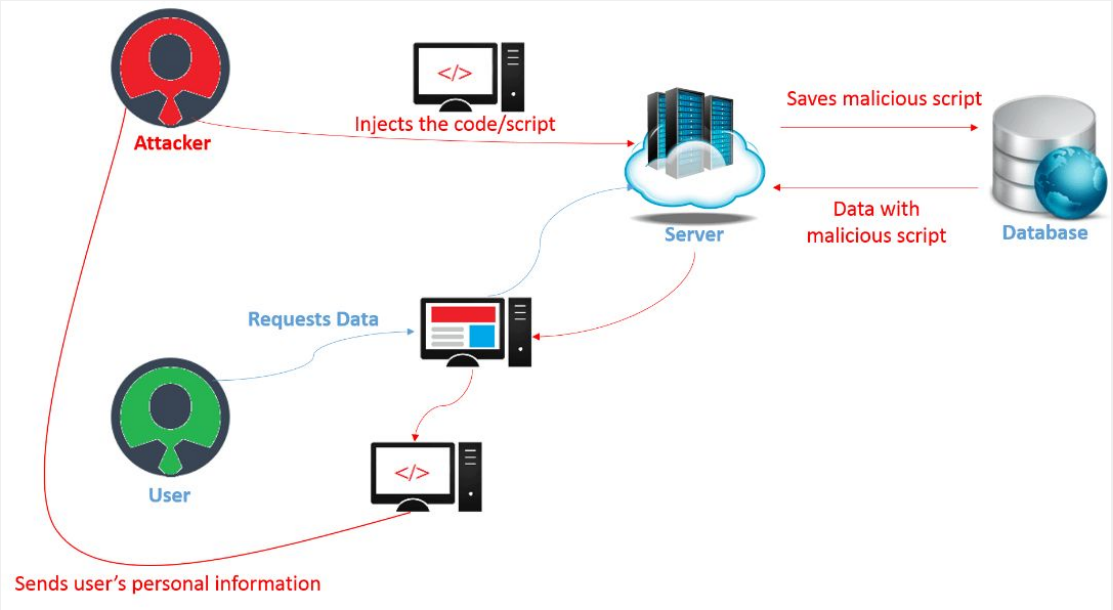
A kind of attack carried out when the user is logged into a session **(or account**) and a hacker uses this opportunity to send then a forged HTTP request to collect their cookie information.This is because,in most cases the cookie remains valid as long as the user or attacker remains logged in to the account.After successfully compromising the user's session,the hacker generates requests to the application that will not be able to differentiate between a valid user and a hacker;because the server is already confused.



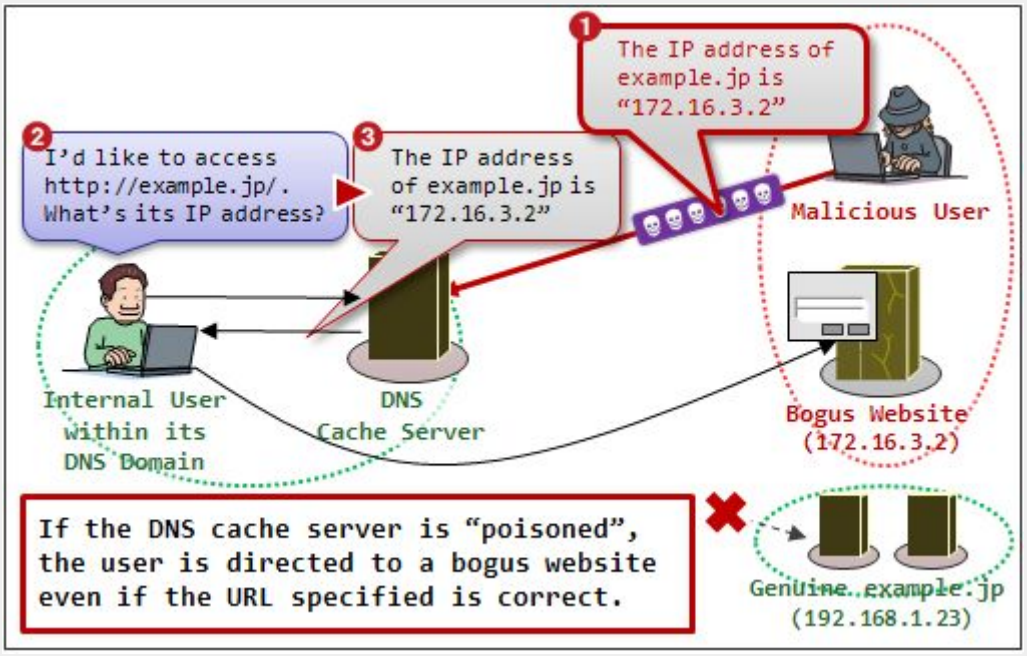
(b) Cross Site Scripting attacks/XSS Attack



Occurs when an application,URL- "get request",or file packet is sent to the web browser window whilst bypassing the validation process.The hacker will run commands that cause the user's **session ID** to be sent to the attacker's website; allowing him to hijack the user's current session and if he gets the cookie(as in cross site request forgery attack),he makes the browser believe he is the legitimate user thus carrying out identity theft.An XSS script deceptive property makes victims believe that a compromised page is actually **legitimate** and **genuine**.The user might see a pop-up window asking for sensitive and personal info-even though the actual website is not the one behind this action.

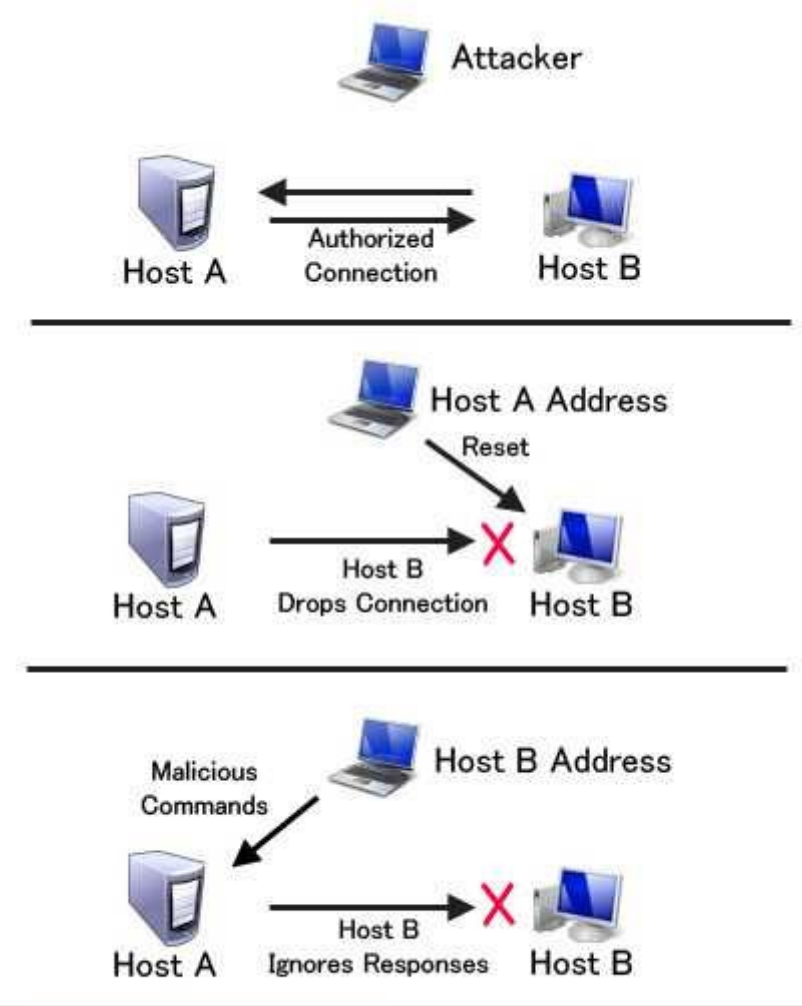


(2)DNS(Domain Name System) cache poisoning or **DNS spoofing** involving old cache data on your browser that you think you no longer need but it can actually be exploited.Attackers will identify vulnerabilities in a DNS where they divert traffic from legit servers to a fake website or other servers.This kind of attack can be replicated and sent to another DNS,therefore poisoning everything it comes across.



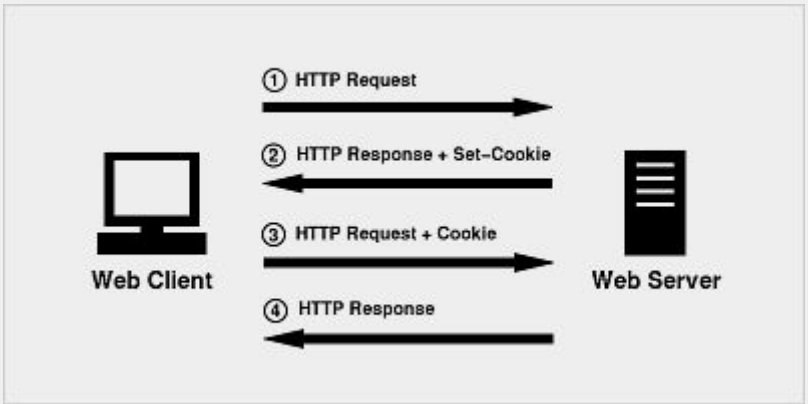
(3)Broken Authentication Session

Authentication systems deal with passwords,key management,session IDs and cookies.These allow a hacker to access your account from anywhere as long as these authentication systems are still valid.If a hacker exploits them then he will assume the user's identity.



Solution:

HTTP Cookies



Most websites use cookies as the only identifiers for user sessions,because other methods of identifying web users have limitations and vulnerabilities.If a website uses cookies as session identifiers,attackers can impersonate users' requests by stealing a full set of victims' cookies.From the web server's point of view,a request from an attacker that has the same authentication as the

victim's requests,there is no distinction;the request is thus performed on behalf of the victim's session.For instance,replaying a cookie,session ID,a Kerberos ticket,an authenticated session,or another resource that authenticates the user after the password authentication process,an attacker can access the password protected resource without ever knowing the password.This is usually the case when the user does not log out or some websites do not have time-outs whereby if your account has been inactive for a period of time deemed to be too long you're automatically logged out.So,someone on the network who could gain access to the same website or application wouldn't be able to use any type of your authentication credentials mentioned above to gain access.This **vulnerability** is most prevalent to websites that use **HTTP Cookies**.Forged cookies and session hijacking is a serious issue- in Mid July 2017,**Yahoo** revealed that during the past 2 years 32 Million User Accounts had being compromised using forged cookies.

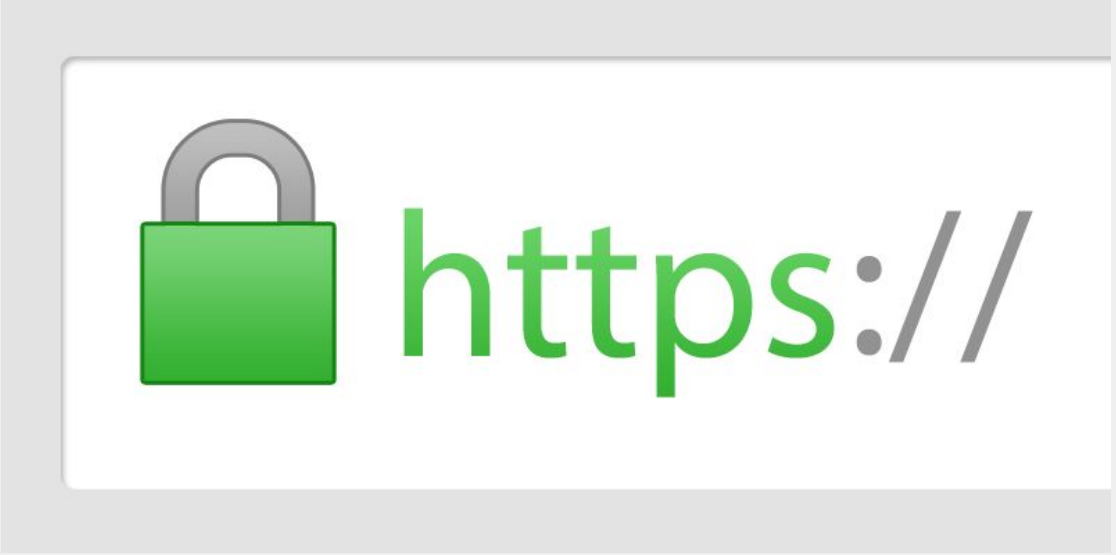


Solution:

Using HTTPS

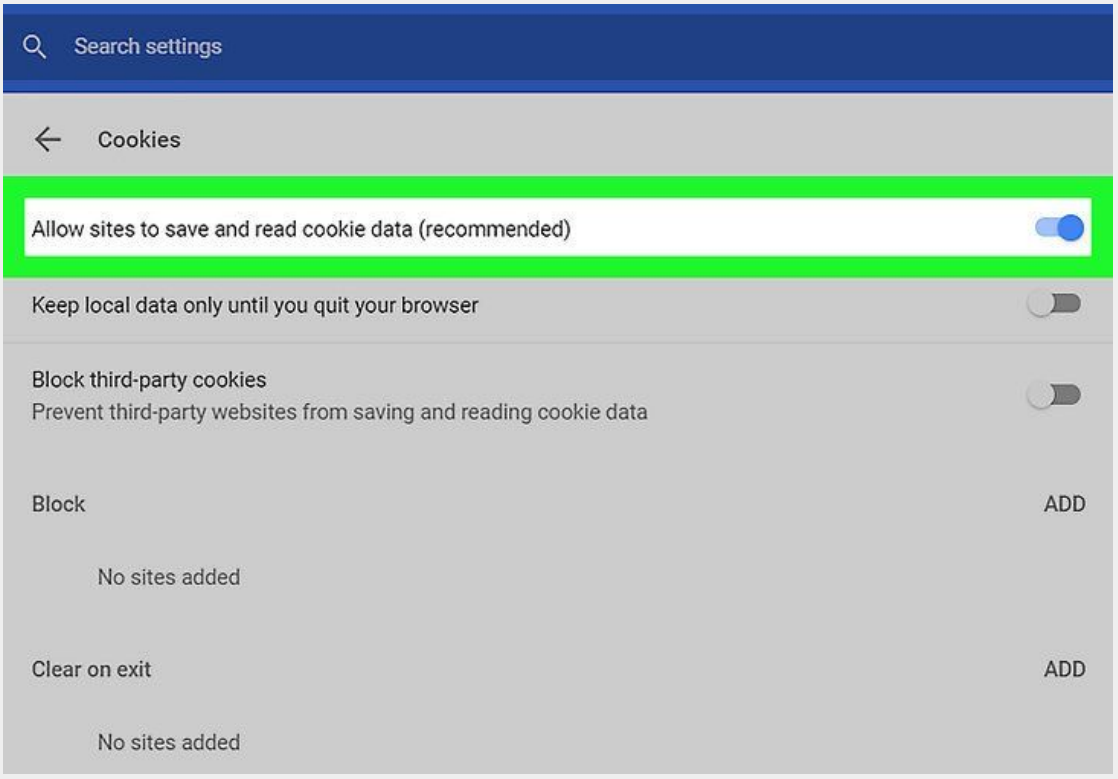


(**Secure HTTP**) across the entire site can prevent session hijacking.Using SSL Certificates can not provide enough security.The Secure HTTP is represented by a padlock icon on the top left corner of the address bar;to mean that the data being exchanged on these pages is secure.Once the user is authenticated to the site,no further communication should take place over HTTP,including loading other content.This measure would also be used to prevent Man-in-the-browser who could try and access the data as it is in transit.





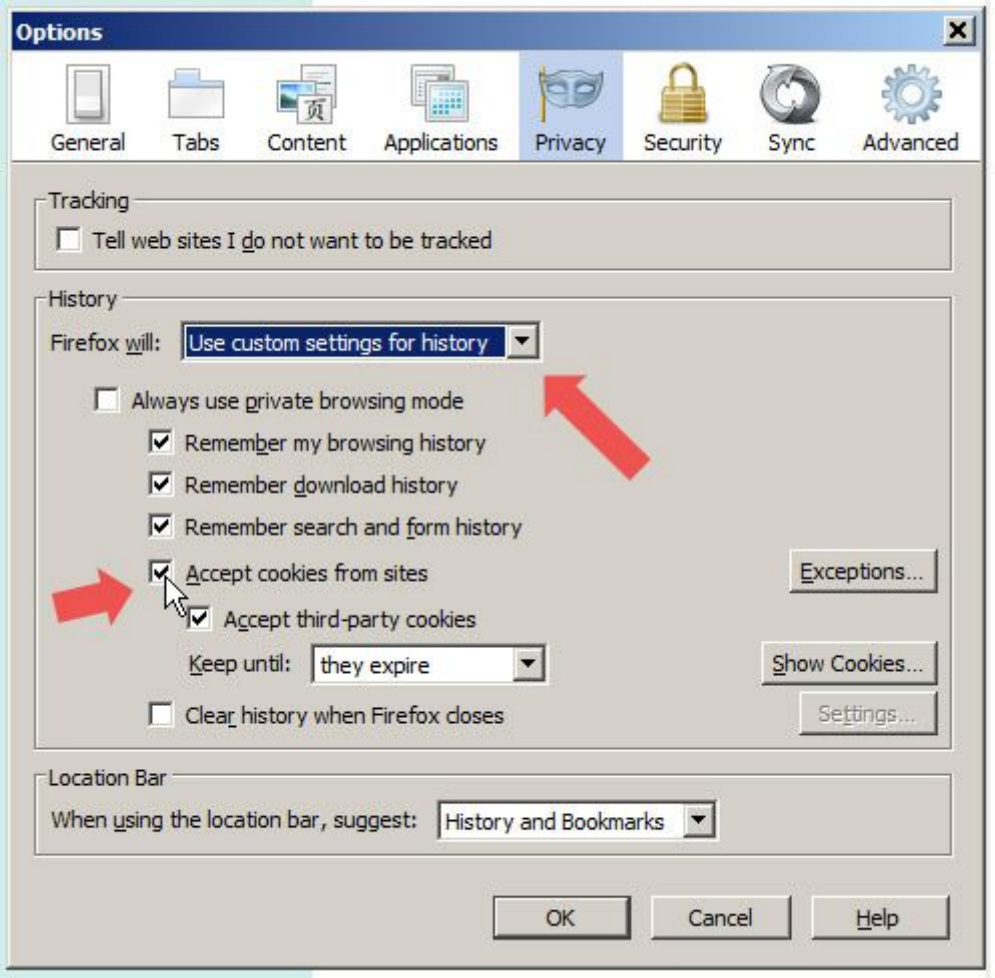
Disabling Cookies



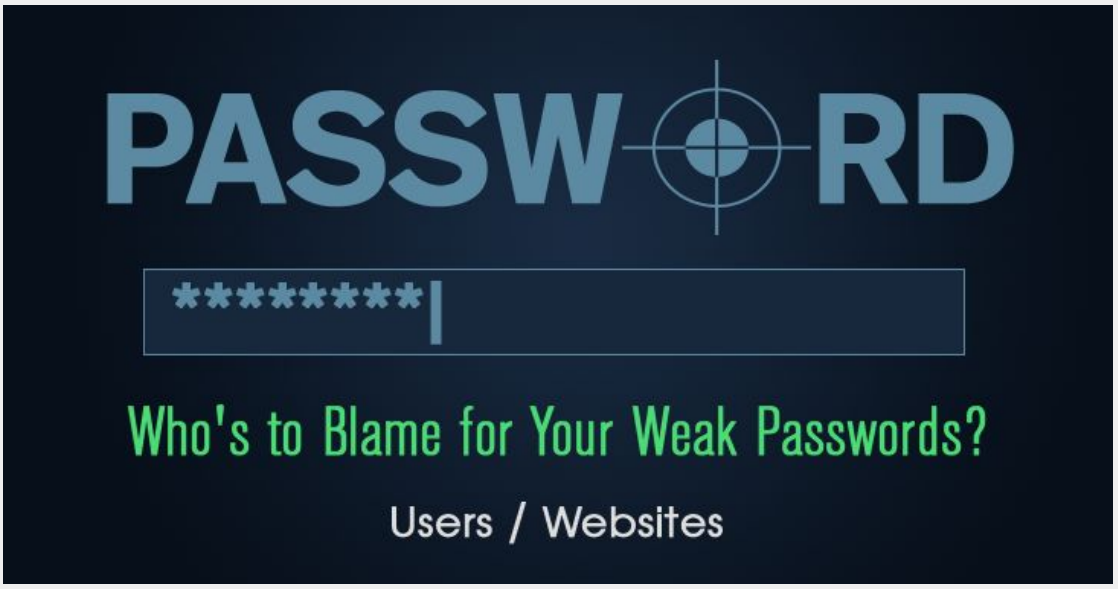
This is done to prevent tracker cookies(**persistent cookies**) in most cases.More Tech Savvy user's will disable cookies to prevent cookie-stealing and session hijacking because of the vulnerabilities that come about with cookies.Sometimes,they disable cookies unknowingly i.e On the Security or Privacy settings on the browsers they move the bar from "medium" to "high" and this automatically disables cookies.However,disabling cookies leaves websites broken and they cannot function;you will not be able to access online services because they cannot identify you and serve you.This leads to users thinking that the browsers are the broken ones and get others but this doesn't solve the problem either,if they still disable cookies.A majority of sites rely on cookies,despite the availability of other authentication mechanisms,for instance **Facebook** and **Twitter** do not work without Cookies.Users will however disable cookies for increased Privacy and Security especially when visiting certain unscrupulous sites.

To deal with the downside of disabling Cookies,users should be made to

understand that only session cookies are needed for session management within the web application and it's possible to automatically erase all cookies when the user closes the browser.



Poor Password Policies



Most websites do not do a lot in terms of enforcing proper secure passwords on the user's.User's cannot be trusted to come up with secure passwords and in any given system there will be a certain percentage of user's who use bad passwords.Password properties such as length,numbers,uppercase and lowercase letters,symbols and charset size or abstinence from common password types are more often than not overlooked or not fully implemented.Most of the sites just require user's to input an 8 minimum character password and it should at least consists of a symbol,number and an uppercase letter.This is good but not enough,for example we all know that numbers,symbols and Uppercase letters are usually appended at the beginning or at the end;what do the computer systems do if you make such a mistake?Absolutely Nothing.It is pointless for us to stay still and watch people make the same mistakes every time and still expect that password security will increase,Insanity isn't any different from what we would be doing.We ought to learn from past data breaches and mistakes,common sense dictates that! Computer systems should be programmed in a way to refuse passwords with such common mistakes that time and advances in technology have outlived.

Solution:

Websites ought to enforce tight and more strict password policies,whilst educating the user's on the importance of strong passwords to avoy feet dragging and reluctance from the user's because we have said that the human mind doesn't like pressure.

(I)Minimum password length of 13 characters.
(II)Have at least one number and NOT at the beginning or at the end.
(III)Have an uppercase letter but NOT appended at the beginning or at the end.
(IV)Have at least one symbol appended NOT at the beginning or at the end.
(V)Meet most of the charset size threshold (a-z,A-Z,0-9)Symbols Unicode class letter-like symbols.
(VI)The password shouldn't be among the most common passwords or in any

of the password blacklists.
(VII)In case the user opens an account,it is wrong to send passwords via email or phone because they can be tapped.Even if end-to-end encryption was employed;it is not that secure plus some encryption algorithms are easily decrypted by hackers.

(VIII)There should be regular password auditing to make sure the passwords meet all the requirements and prompt users to change theirs if found to be too weak(and this has to be enforced to the latter).After a data breach in Yahoo back in 2013,some passwords were breached and those that were weaker than those in 2013;were breached in December 2014.This would not have happened if the users had been encouraged to strengthen their passwords.I know that this might be a bit of pressure to the user's but it is worth the effort because it gives an added layer of security.The websites could also tweak some of these policies depending on the sensitivity of some sites e.g a bank(all should apply) and maybe a book reading site which in all honesty doesn't have any sensitive content that could be attract attackers.Bruce Schneider,a renowned security expert advises people to come up with complex passwords and write them on a piece of paper,then put them in their purses and wallets(they are very private areas) and then after memorizing them and recalling them comfortably,they can do away with the pieces of paper.I think this is a good move to compliment the better password policies.

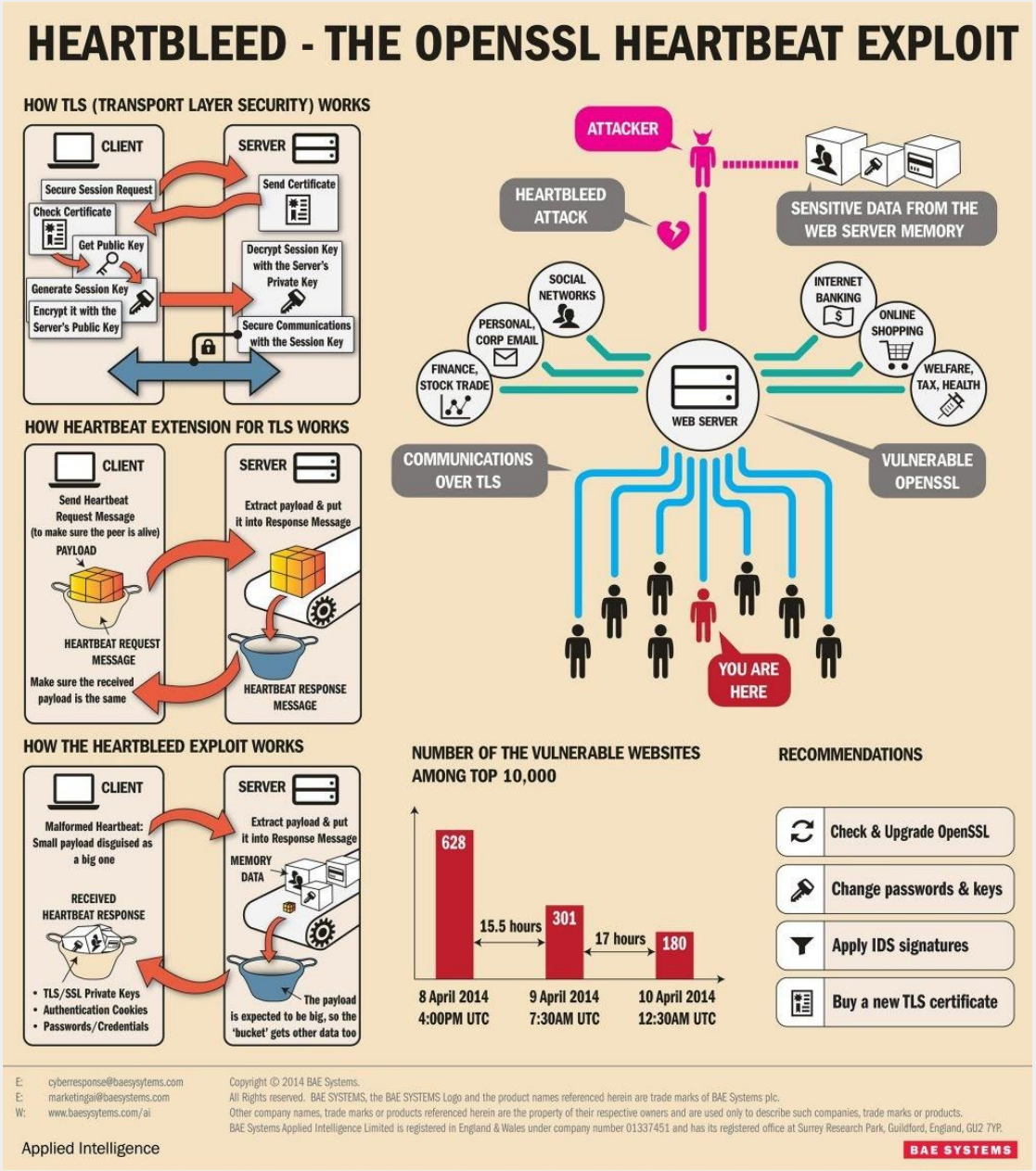
Data Breaches



Over the past few years and especially from 2010 to now,there have been many prominent cases of hackers gaining access to large amounts of personal information from major data breaches,especially passwords.Most of these leaked data is readily available on the web for anyone to exploit.Most of these breaches done through compromising databases(**as we saw in Chapter 3**).What happens in the aftermath of such events is that the service will notify everyone whose data was breached,allowing them time to decrypt the password database.For anyone maintaining good practice such as shunning

password re-use across accounts and paying attention to events in the tech world,it will be easy for them to adapt to the situation.It becomes most problematic,though for the large(**really large**) number of people who don't follow good practices.A good example of data breach notification;The Heartbleed Bug.

The Heartbleed Bug



A vulnerability that deals with Servers where passwords have been stored.The mechanics behind it is that a cracker will be able to extract information from a server's memory- Be it Cookies,Personally Identifiable Info(**PII**) to aid in identity theft,Authentication Credentials or even the server's private key(even an admin password).Open SSL is an encryption library used in HTTPS(secure HTTP).As those who are observant enough(on the address bar),nowadays if you type the address "www.google.com" it automatically changes to " https://www.google.com".Its function is to encrypt all communication between the server and the client while taking place through the HTTPS URL.Through this the password sniffing,cookie stealing hacks are rendered impossible.During communication,Open SSL uses a handshake or as popularly known,a "heartbeat" that echoes back a signal to verify that the data was received correctly.This is a way of double checking whether the message was successfully received or not(just like the two ticks marks seen on WhatsApp messages).The heartbleed bug vulnerability enables a hacker to trick OpenSSL by sending a message that is misinterpreted by the server that is running the OpenSSL,and which then actually sends back the actual data without any questions asked.A single byte of data maybe sent to the server telling it that it is actually 64 k bytes of data(**the buggy requests work to confuse the server**).The server will then send back 64k bytes of data to be checked and echoed back.After this 'heartbeat',the server again sends back 64k of random data from its memory.The 1 byte containing the buggy requests ends up confusing the server,making it give up random information. With every 'heartbeat'-->64 KB of private information is given away i.e 64,000 characters in the form of plain unencrypted text.

Most of this 64,000 characters might be useless but it may still contain:

I)Accounts
II)Passwords
III)Credit Card Numbers
IV)Cookies
V)The server's private key(even the administrator password)
VI)Personally Identifiable Info(PII)
VII)Any other Authentication credentials

This vulnerability will allow an attacker to do a lot of harm with the information he now has on his hands;identity theft is just a tip of the iceberg.The vulnerability on the Open SSL protocol was patched on 7th April 2014-->The heartbleed bug and in which over half a million web servers were found to be vulnerable!.The who's who(the Internet Giants) on the web and the biggest websites on the Internet were vulnerable:

1)**Google**
2)**Facebook**
3)**Twitter**
4)**Yahoo**
5)**Instagram**
6)**Pinterest**

7)**Dropbox**
8)**Tumblr among others...**

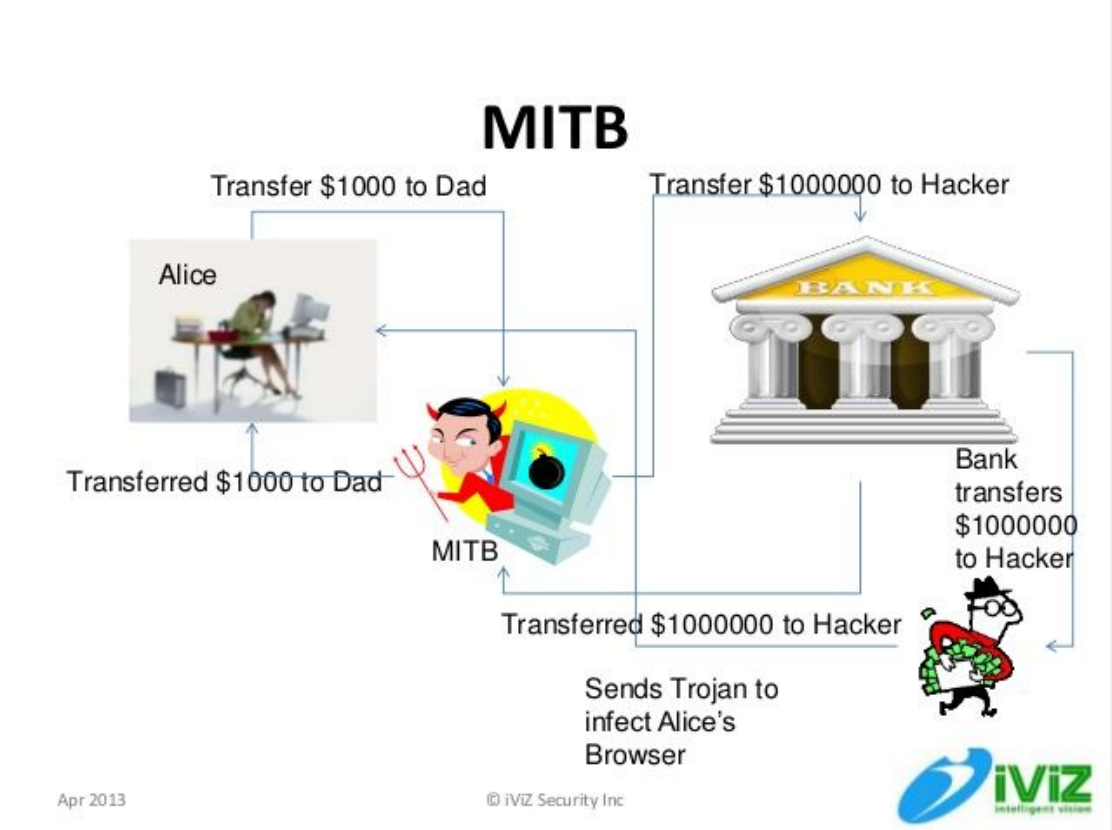
*The websites were quick to announce(**that is within a few weeks time**);that they've successfully patched the bug.However,they did not tell the world that this vulnerability had existed for more than 2 years!!! but had only come to light at that moment.*This is the main reason why users on mainstream social networks and online sites were asked to change passwords.In the wake of **Edward Snowden's** revelations,I wouldn't be surprised to find out that perhaps someone has been using this vulnerability for years to exploit websites.The fact that this vulnerability is still out there means that it can be exploited again,mainly because not all websites have released security patches to solve it.There is even a page on the web that lists the names of thousands of vulnerable websites.



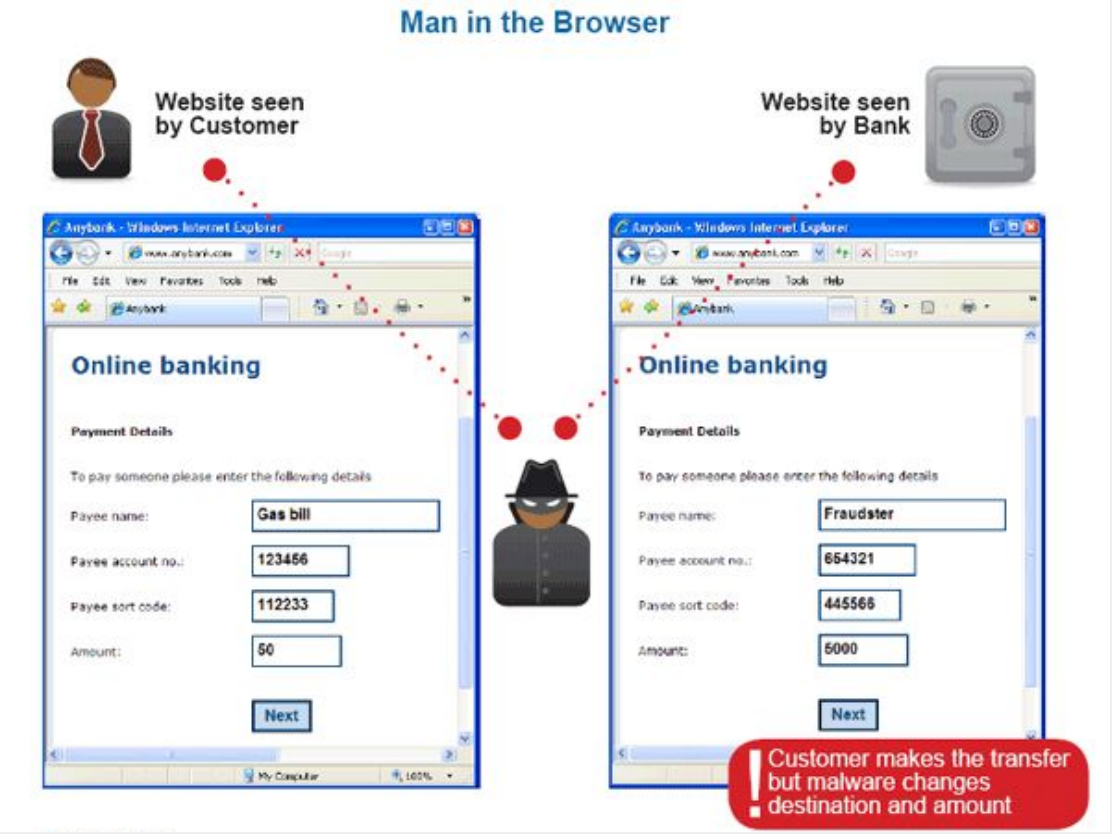
Solution:

The companies did very well in informing user's on time.This is the right thing to safeguard the user from risk of compromise.Some sites however may not notify user's on time and it is up to us to **pay attention** to **data breaches** and happenings across the tech world,we ought to note that there is a list of sites still vulnerable and who haven't rectified the vulnerability.I also take issue with the fact that this vulnerability had been in existence for two years before the exploit,the websites new but didn't tell us.In the current world,hackers won't take 2 years to exploit a **vulnerability**,they are getting more and more advanced by the day.They have forums and groups to share information.Leaked data from breaches is also being shared with everyone on the web.The websites were lucky in the case of the Heartbleed bug...I think they should act much sooner in the future.

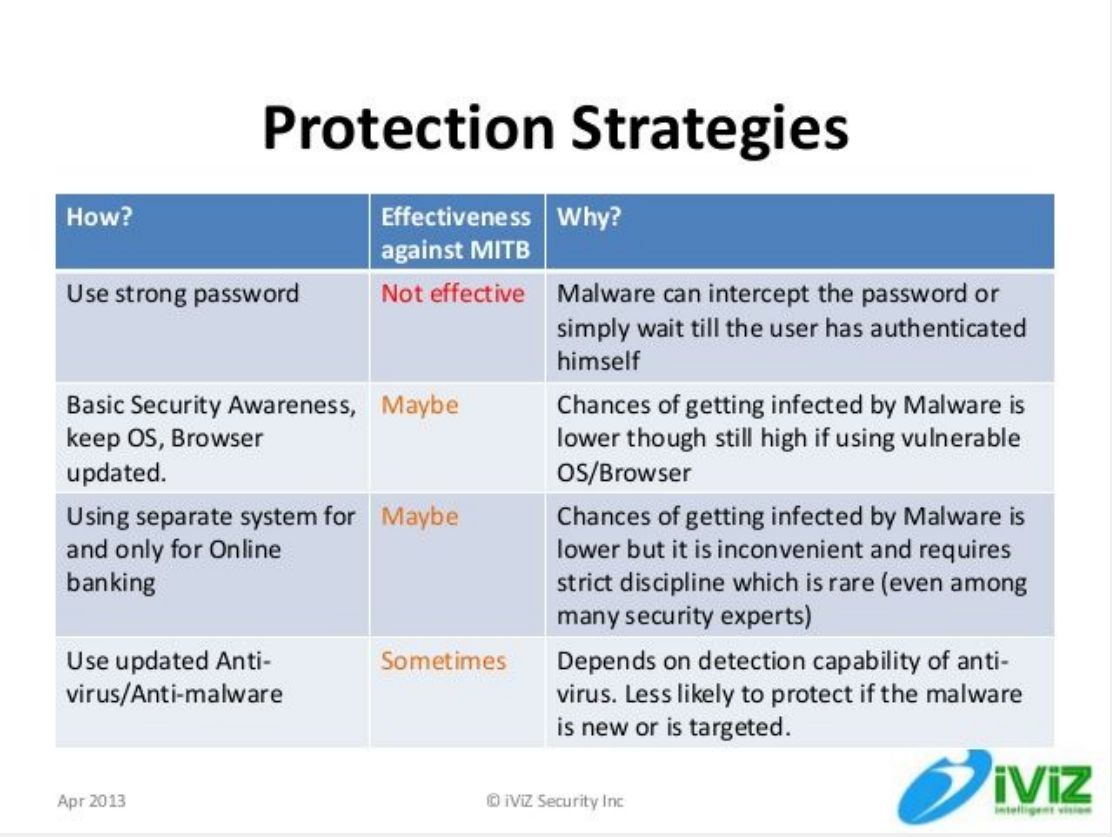
Man-in-the browser attacks



Usually abbreviated as MITB,MitB,MIB or MiB is a form of internet threat related to man-in-the middle(MITM) and is a proxy Trojan Horse that infects a web browser by taking advantage of vulnerabilities in browser security to modify the web pages,modify transaction content or insert additional transactions in a covert fashion invisible to the user and host web application.**Trojan Horse->**A software that appears to perform a desirable function for the user prior to it running or installing on a device but later steals information or harms the system.Some of the mischief a Trojan Horse can cause is messing with the user's interface,erasing files,capturing keystrokes and stealing passwords and even taking control of your mouse! MitBs are in most cases successful despite the added layer of security that is two/three factor authentication,PK and SSL security mechanisms.There have been various challenges dealing with MITBs;Malicious extensions live only in the browser and don't have any indicators of compromise leave traces in critical system areas making it hard for antivirus software to detect them,Malicious extensions and harmful scripts can look legal and the user cannot tell the difference moreover,the malicious code reside on remote servers and not on the PC amongst other challenges.In the early days Internet Explorer(a feature known as BHO-Browser Helper Objects that deals with browser extensions and user scripts like **JavaScript**,however **Microsoft** has solved the issue by making sure BHOs are digitally signed off) and **Firefox** browsers were the most vulnerable browsers but nowadays nearly all if not all browsers are vulnerable(i.e **Chrome,Opera,Safari,Netscape** and **others**).



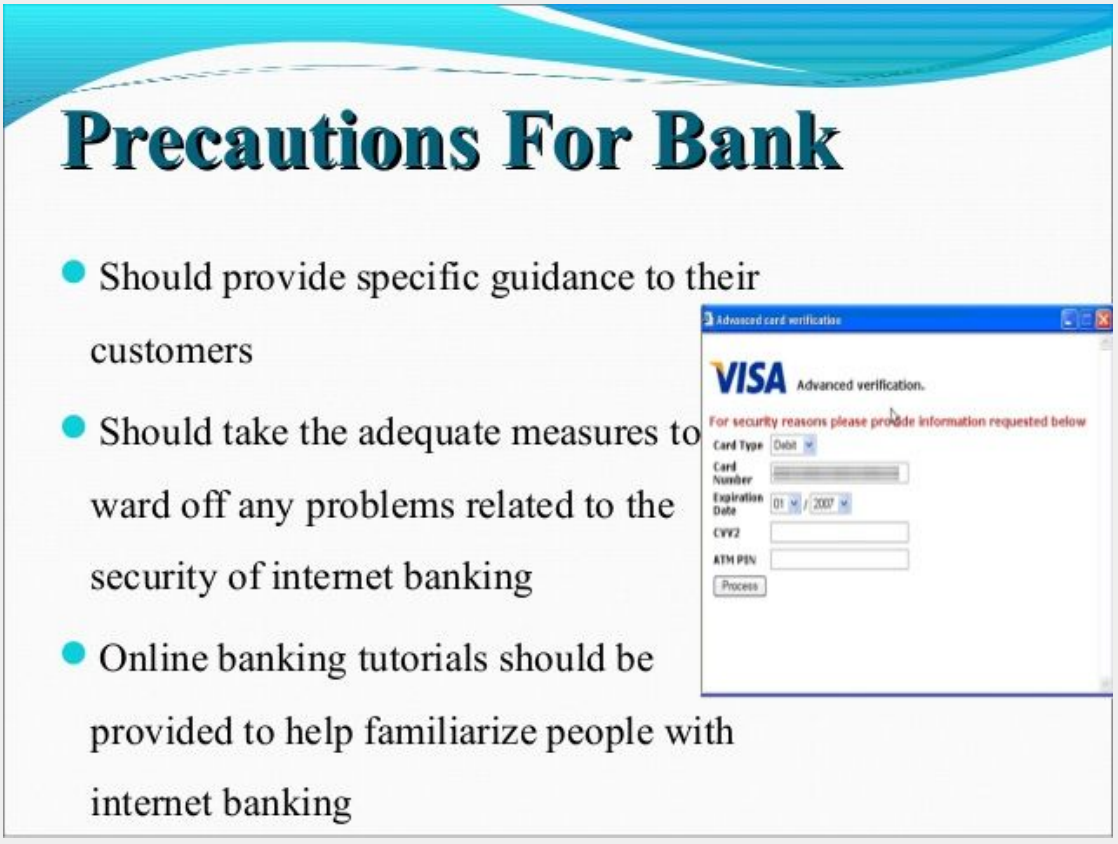
Protection against MitB



1)Installation of Antivirus software
2)Use of browsers with additional security mechanisms-such as those with an

in-built blacklist of malicious extensions.

3)Artificial Intelligence **(AI)** and machine learning within browsers to be able to prevent users from entering websites with malicious extensions in the first place.Other techniques include Server-side techniques incorporating Content Secure Policies(CSP).



Safeguards

How?	Effectiveness against MITB	Why?
Enforce strong password	Not effective	Malware can intercept the password or simply wait till the user has authenticated himself
Using Encryption, eg, SSL or client side encryption of password/transaction details	Not effective	Malware can intercept and modify the request/response
Multi-factor authentication, eg, Biometric/OTP/Smart Card	Not effective	Malware can simply wait till the user has authenticated himself.
CSRF Tokens, Frame-buster, Challenge response/captcha, etc	Not effective	

Phishing

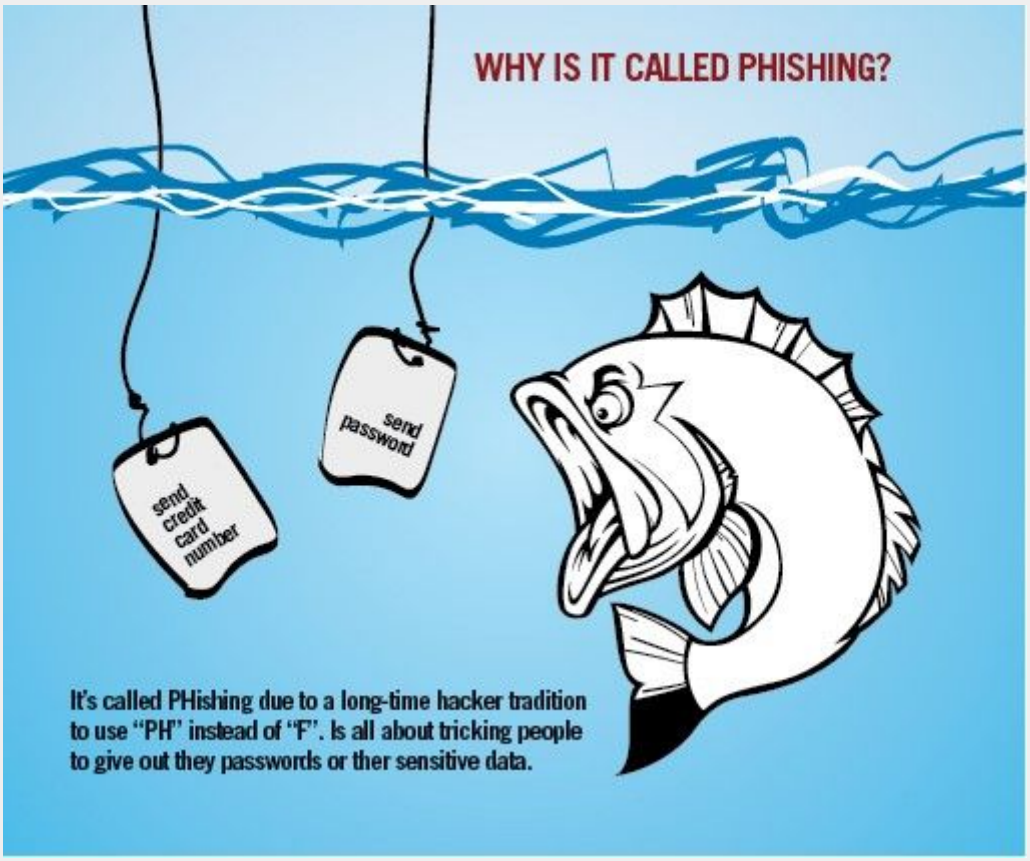


This is attempting to acquire information such as usernames,passwords and even credit card details by masquerading as a trustworthy entity in electronic communication.It can also be considered a form of social engineering since it preys on and takes advantage of the victim's trust.Communication purporting to be from popular social websites and online payment processors amongst others are commonly used to lure the unsuspecting user.Phishing is typically carried out by email spoofing or instant messaging,and it prompts the user to enter his/her details (i.e sensitive information like your password,bank account or credit card details)at a fake website whose look and feel are almost identical to the legitimate one.Most of these fake emails and communication threaten that your account will be in jeopardy if you do not take action immediately.An email that urgently requests you to supply sensitive personal information is usually an attempt at fraud.Also,**fake emails** often contain misspellings and grammatical errors or are written in a language which you did not set as the preferred one for your account when you signed up.





Anthem,a company based in the **United States** in February 2015,was compromised.Personal information of more than 78.8 Million Customers stolen with the breach allegedly starting a year earlier;when a single user at an Anthem Subsidiary had clicked on a link in a Phishing Email.Another instance is that of **RSA Security**,a security firm based in the **US** in March 2011.Nearly 40 Million employee records were stolen.The attack was Carried out via phishing.Attackers posed as people the RSA Employees knew and trusted.They were then able to penetrate the company's network(and the rest is history).



Solution:



Make sure that the website you are giving your account and password to is a verified and genuine site by simply peeking at the address bar in your web browser(which I know most of us overlook).This is because you cannot fake the address.It is also good to avoid following any links from any dodgy and

suspicious websites,scam
emails or even the comment sections in various places.Online Services should constantly remind their clients to be vigilant about Phishing attacks while giving them the signs to look out for like **Paypal** does in some of its emails.



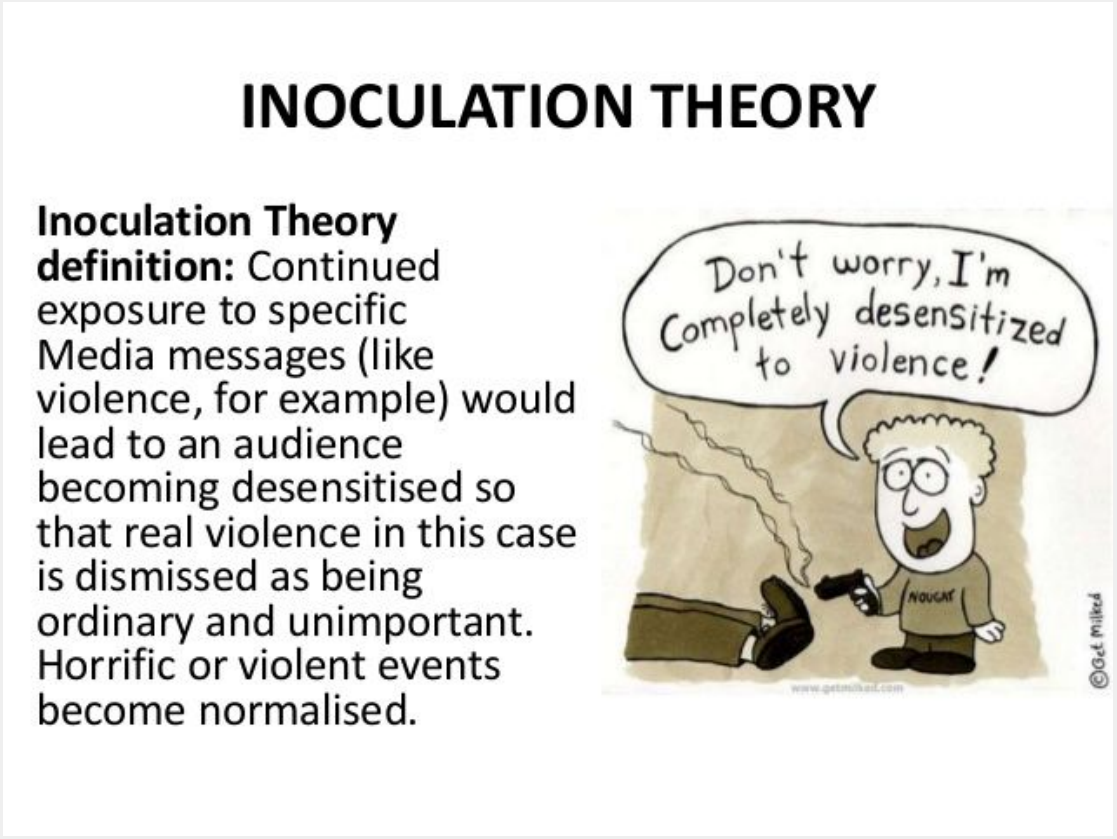
Social Engineering



A **nontechnical** kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security practices.In other words Social Engineering aims to convince a user to disclose secrets such as passwords,credit card numbers etc. by impersonating as a customer support associate,a bank or even a customer.Appeal to Authority,Appeal to Vanity and Old-fashioned eavesdropping are some other forms of Social Engineering The user is made to give up vital information in a casual conversation.The information might be the user's recovery question's answer,and which can then be used to take over the account via things like: "Forgot Your Password?Click Here" Button.Social engineers run "**con games**",in that they pretend to be helping the user but they have ulterior motives,they rely on the natural helpfulness of people as well as their weaknesses.They might call the authorized employee with some kind of urgent problem that requires immediate network access.A while back,**Facebook** rolled out a 24 hour delay before recovering the account and logging in if one had forgotten the password(I don't know if this practice is still in place).For the hacker,such an exploit requires a lot of planning and timing,because if the user happens to log in during that period,the whole process can be reversed in a couple of seconds.Furthermore,Facebook uses a verification method during recovery-if the user's email and phone number are no longer available/functional it asks for another phone number.If the hacker can somehow manage to get a hold of the victim's phone or email account,they have succeeded in taking over the account.



Solution:

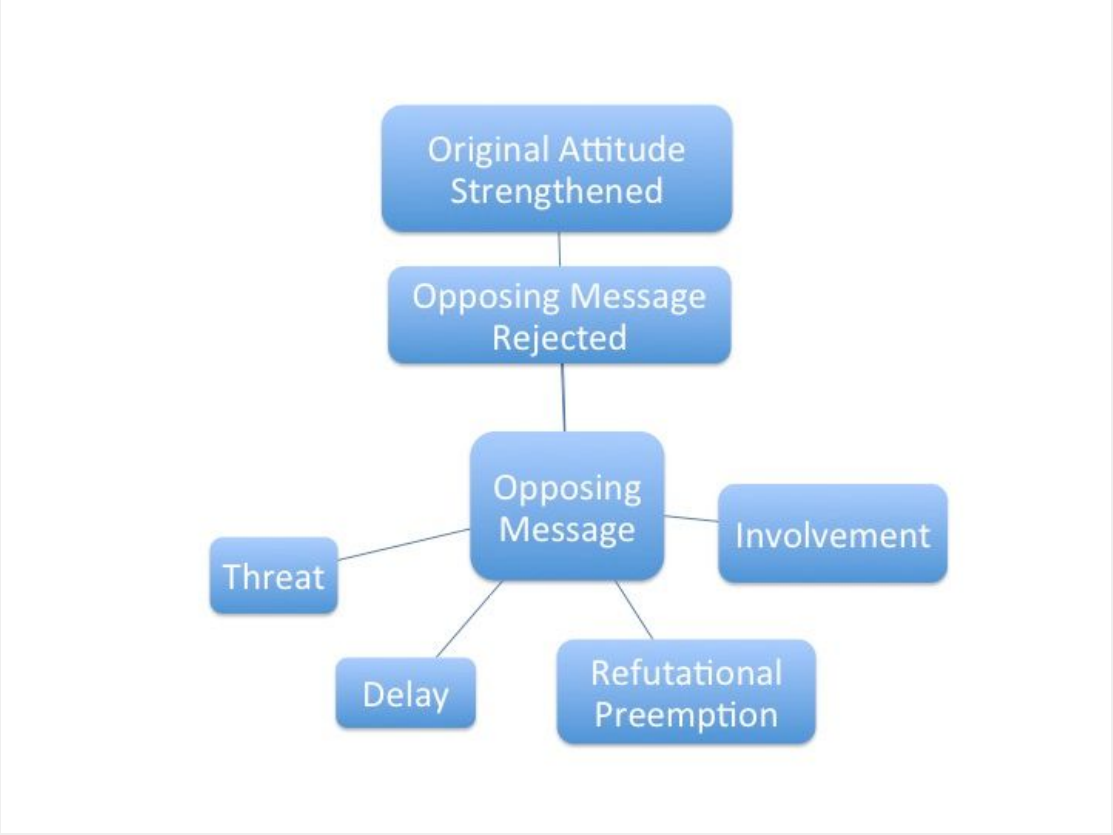


Enoculation(Derived from The **Inoculation theory)-** seeks to prevent social engineering and other fraudulent tricks or traps by insisting a resistance to persuasion attempts through exposure to similar or related attempts.

Inoculation Theory: States that to prevent persuasion it is necessary to strengthen pre existing attitudes,beliefs,or opinions.First,the receiver must be

made aware of the potential vulnerability of an existing position (e.g., attitude, belief).This establishes threat and initiates defenses to future attacks.The idea is that when a weak argument is presented in the inoculation message,processes of refutation or other means of protection will prepare for stronger arguments later.It is critical that the attack is strong enough to keep the receiver defensive, but weak enough to not actually change those preexisting ideas.Treglia and Delia (2017) apply inoculation theory to cyber security; people are susceptible to electronic or physical tricks,scams or misrepresentations that may lead to deviating from security procedures and practices,opening the operator,organization or system to exploits, malware,theft of data or disruption of systems and services.Inoculation,or enoculation,in this area improves people's resistance to such attacks,examples and directions for future work are provided.

This theory when applied to **prevent** Social Engineering means that users will be first educated on the dangers of social engineering attacks and are made to understand how the social engineers might try to convince him to do what they want.After subjecting the user to such scenarios in theory then it helps to build up the psyche up the user and his reflexes not to give in to such attacks in case they do actually happen.

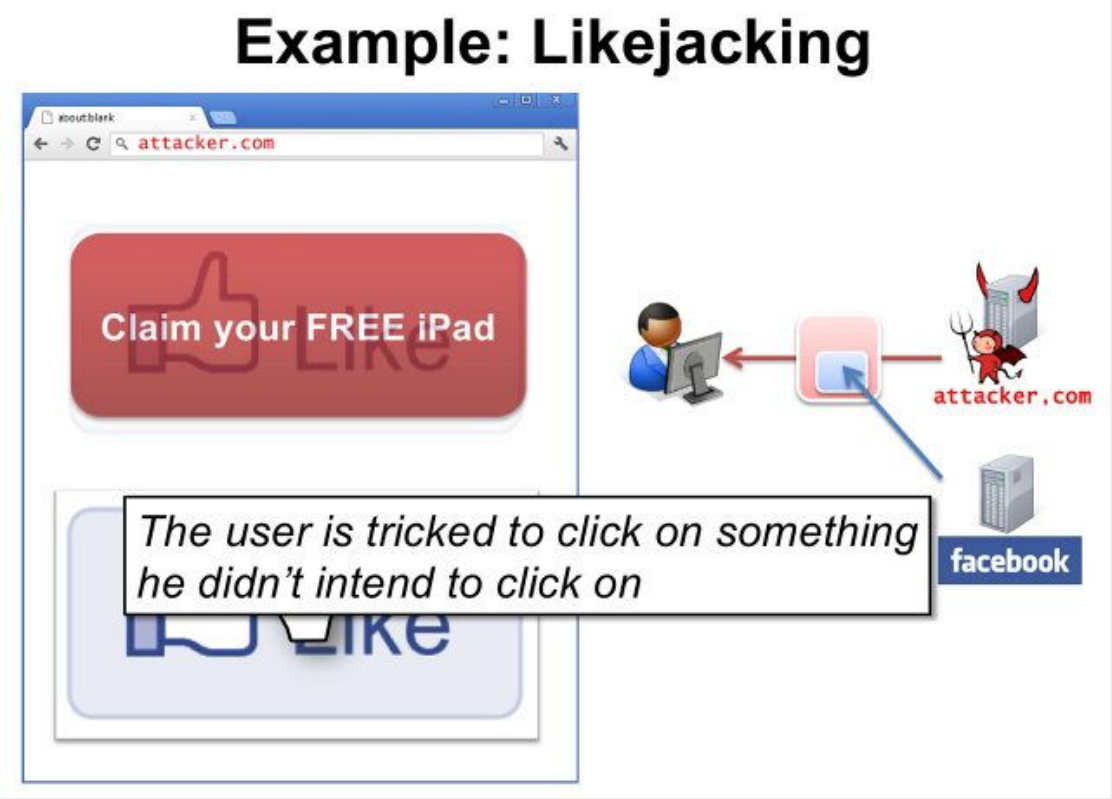


Clickjacking



Clickjacking which is also known as "UI redress attack" i.e "User Interface attack" is a malicious technique in which as the name suggests,deals with a user interface.It is a kind of confusion technique.An attacker tricks a user into clicking on a button or link on another web page while the user initially intended to click on the top level page.The attacker is basically "hijacking" the clicks meant for the top level page and **routing them to some other irrelevant page,most likely owned by someone else**.A similar technique is hijacking **keystrokes**.An attacker will carefully draft a combination of stylesheets,iframes,buttons and text boxes.The user will then be made to believe that they are typing the password or other information into an authentic webpage but this isn't actually the case because the information is being channeled into an invisible frame controlled by the attacker.

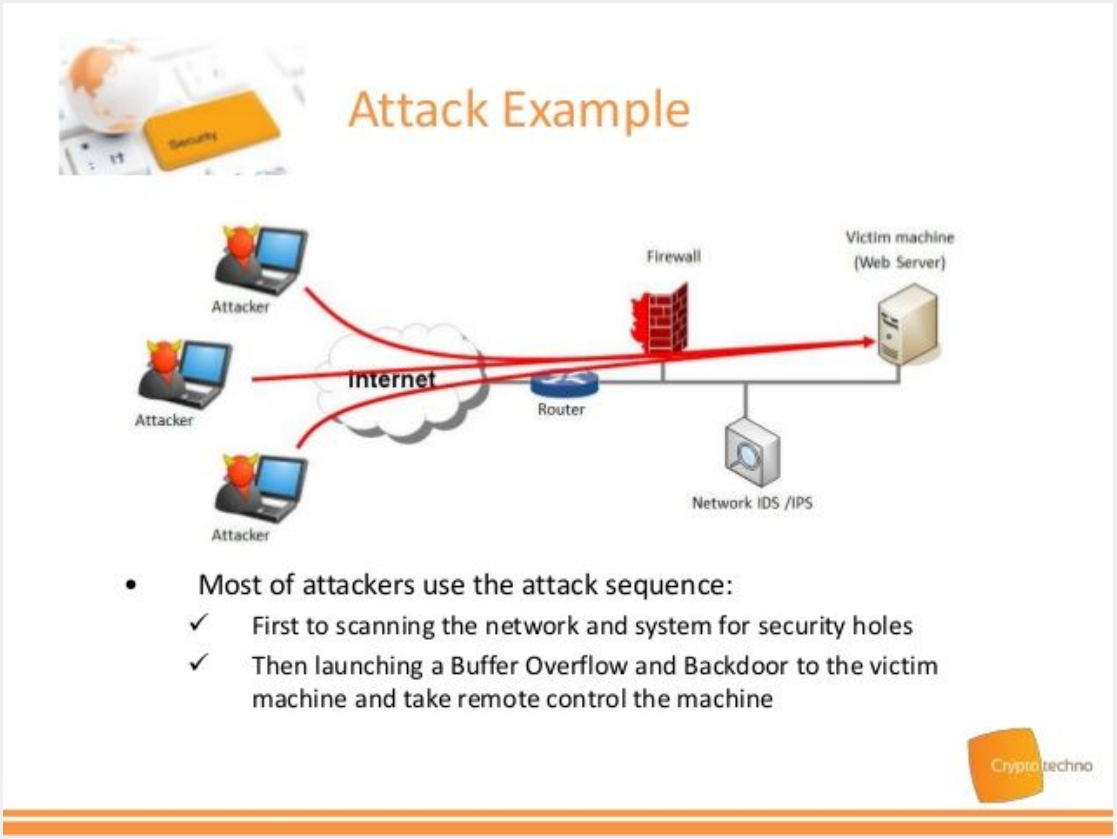




Backdoors



A backdoor is using a cryptosystem or an algorithm or any secret method to bypass normal authentication or security checks and controls. They may exist for a number of reasons;from original design by the security engineers and penetration testers to poor configuration.They may also stem from the addition by an authorized party to allow legitimate access,or by an attacker for malicious reasons such as providing a network connection for attackers or malware/viruses and spam to be sent to the user.



Direct Access Attacks



In this case,an unauthorized user gains access to a computer and is able to directly copy data from it.They may also compromise Security by making OS(Operating System) modifications,installing software worms,keyloggers,inserting covert listening devices and using wireless mice.

Direct Access Attack (Physical Theft)

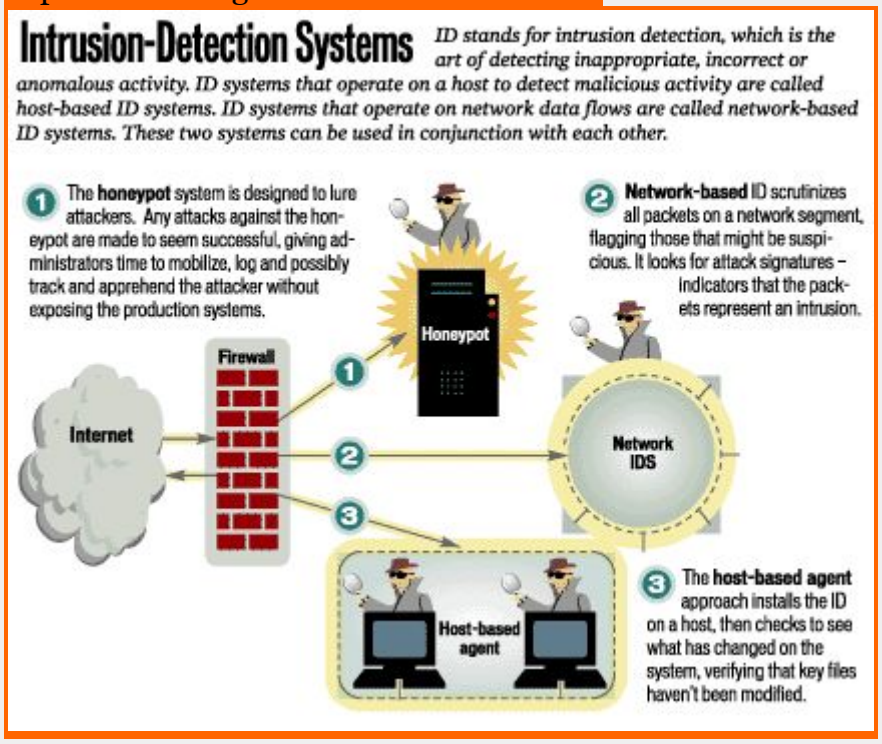
- An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless mice
- Even when the system is protected by standard security measures, these may be able to be by-passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.



Solution:

(a)Drive Locks-These are Software tools to encrypt hard drives and make them inaccessible to thieves.One can also encrypt external drives.

(b)Intrusion Detection Systems(IDS)- These products are designed to detect network attacks in progress and assist in post-attack forensics. Audit trails and logs serve a similar purpose for individual systems.
IDS can scan a network for people that are on the network but who shouldn't be there or are doing things that they should not be doing,such as trying a lot of passwords to gain access to the network.



(c)User Accounts- Access Controls and Cryptography to protect system files and data respectively.

(d)Biometric Validation such as thumbprint readers or QR code reader software designed for mobile devices offer secure ways for mobile phones to access control systems.

(e)USB Dongles- An idea to prevent unauthorized access to a computer or other devices' software.The dongle,or key creates a secure encrypted tunnel between the software application and the key.The principle behind this is that an Advanced Encryption Standard(AES) provides a stronger measure of security,since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and user.What's more interesting is that USB dongles can be configured to lock/unlock a PC.This method is used to complement Disabling USB Ports (works by preventing unauthorized and malicious access to an otherwise secure computer, by preventing the effects of infected USB dongles connected to a network).Dongles can also be used to access web-based control such as Cloud Software or Virtual Private Networks(VPNs).
Among other hardware protection mechanisms.



Eavesdropping



This is a quite common term even away from computers and technology,in

regard to listening to people's private conversations.In computer security,eavesdropping more or less means the same but with a slight twist;it is the act of listening to a private conversation,between hosts on a network.A perfect example is programs such as **Carnivore** and **NarusInsight** which it is widely alleged that they have been used by the **FBI** and **NSA** to eavesdrop on they systems of Internet Service Providers.**TEMPEST**,a specification by the NSA can eavesdrop on **closed systems** i.e systems with no contact to the outside world.This through monitoring the faint electromagnetic transmissions generated by the hardware!Other methods are Tampering,Spoofing and Privilege Escalation.

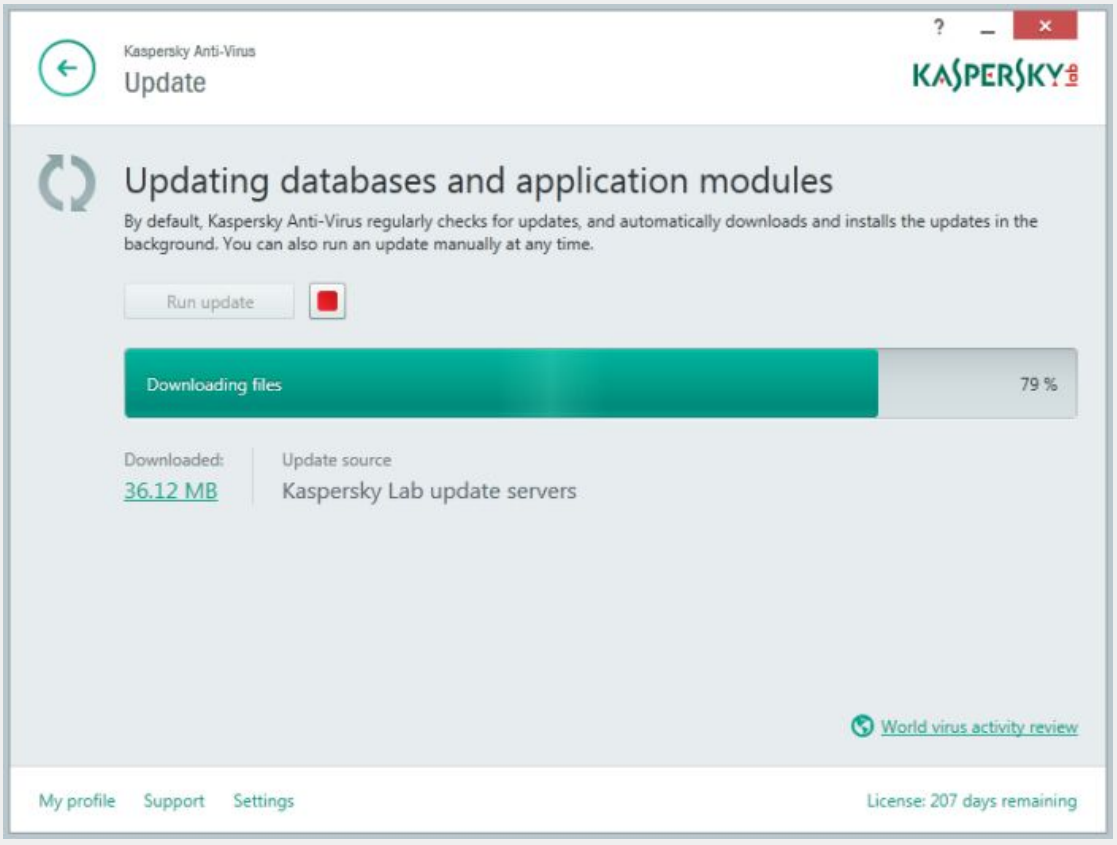


General Solutions

Install & Update Your Antivirus Software



Antivirus software is designed to prevent malicious software programs from embedding on your computer.If it detects malicious code,like a virus or a worm,it works to disarm or remove it.



Methods of Protection from Viruses

1)**Cleaning-** After scanning and detecting a virus program,a good Anti-virus program should be able to clean affected files and prevent the virus from mutating.Most Antivirus software can be set up to scan automatically daily,weekly and monthly(but daily is the best option).

2)**Quarantine-** This is the moving of an infected file such as a virus into an area where it cannot cause any harm.The Quarantine feature helps the user keep up with virus activity.Quarantine basically works by encrypting the virus with a code which makes it useless and nonthreatening.Antivirus programs are good,very good in fact,however they have a downside in that they can give false positive results and make mistakes.That is why Quarantine is important;to keep aside the suspected file until we are completely sure.For those of us who are very observant,you might have noted that the Antivirus database needs to be updated regularly to keep up to date with the codes of new viruses and offer maximum security.It is advised to quarantine a virus for about month before deleting it.



Examples of Antivirus Programs: **AVG,Avast,Kaspersky** amongst a host **others**.



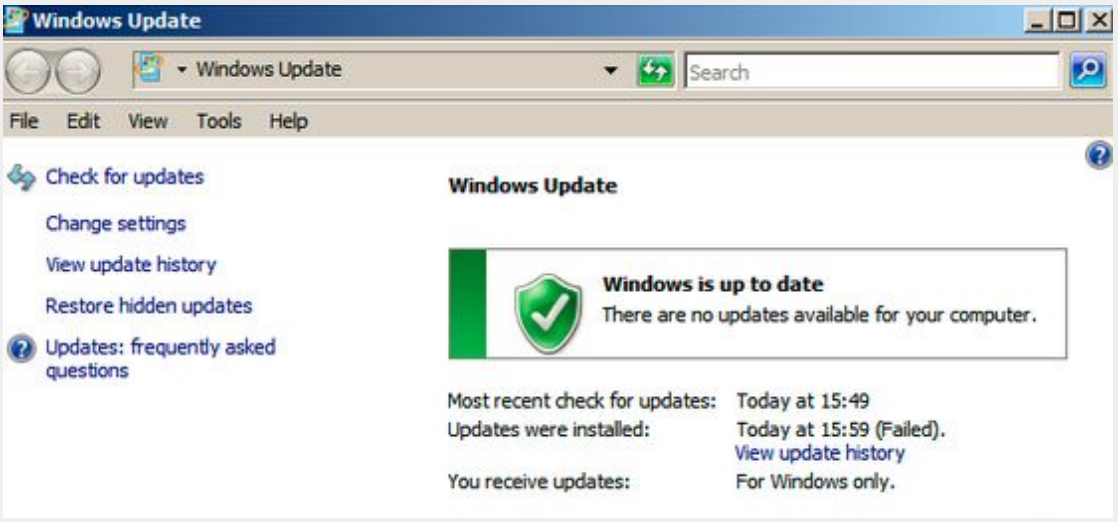
Install & Update AntiSpyware and Antimalware



Spyware is software that is surreptitiously installed on your computer to let others peer into your activities.Spyware collects information about you without your consent.Adware produces unwanted pop-up ads on your web browser which consume the network bandwidth and slow the network connection down.You should be wary of ads on the web offering downloadable antispyware because more often than not they are fake and contain spyware or other malicious code(a classic example of a thief who has been spotted and starts shouting thief instead at the one who saw him)Sometimes spyware such as keyloggers are installed by the owner of a shared corporate or public computer on purpose- in order to secretly monitor others.While the term spyware suggests software that secretly monitors the users computing,the functions of spyware extend beyond simple monitoring.They can collect various types of personal information such as Internet surfing habits,sites visited and can also interfere with user control of the computer in other ways such as Installing Additional Software and Redirecting web browser activity.Spyware has even been known to change computer settings resulting in effects such as Slow Internet connection speeds,Different Homepages,Loss of Internet Connection and interfering with the functionality of other programs.

There are programs which have been developed to detect,quarantine and remove spyware including Adware,Malware bytes and other suspicious programs collectively.**Spyware Doctor** & **Spybot Search** and **Destroy**,Anti-Malware programs,Anti-Spyware programs all work to destroy malware,spyware and adware.Furthermore,almost all commercial Antivirus Software currently detect Adware and Spyware or offer a separate Spyware Detection package.There has been a reluctance to add adware and spyware detection to commercial Anti-virus products,which is fueled by litigation and lawsuits.The best example is between **Kaspersky** and **Zongo** Software.Kaspersky was sued by Zongo for blocking the installation of Zongo's products.This is because Zongo Software and its components are almost universally detected and classified as Adware.

Keep your Operating System Up to Date



Remember Wanna Cry?



Computer Operating Systems are periodically updated to stay in tune with technology requirements and to fix bugs and security holes- install the updates to avoid becoming vulnerable to exploits such as Wanna Cry.You should also have comprehensive data backups and store them somewhere else(**possibly data cloud services**)which is still safe and can still be retrieved easily.It would be sad and incomprehensible to lose all your hard accumulated and precious data at one go.You can also insure your data in case of anything happening to it such as destruction by natural calamities like Floods and Earthquakes,**Hire** competent people responsible for security.Ensure your computer has the latest protection(It is not much to ask).

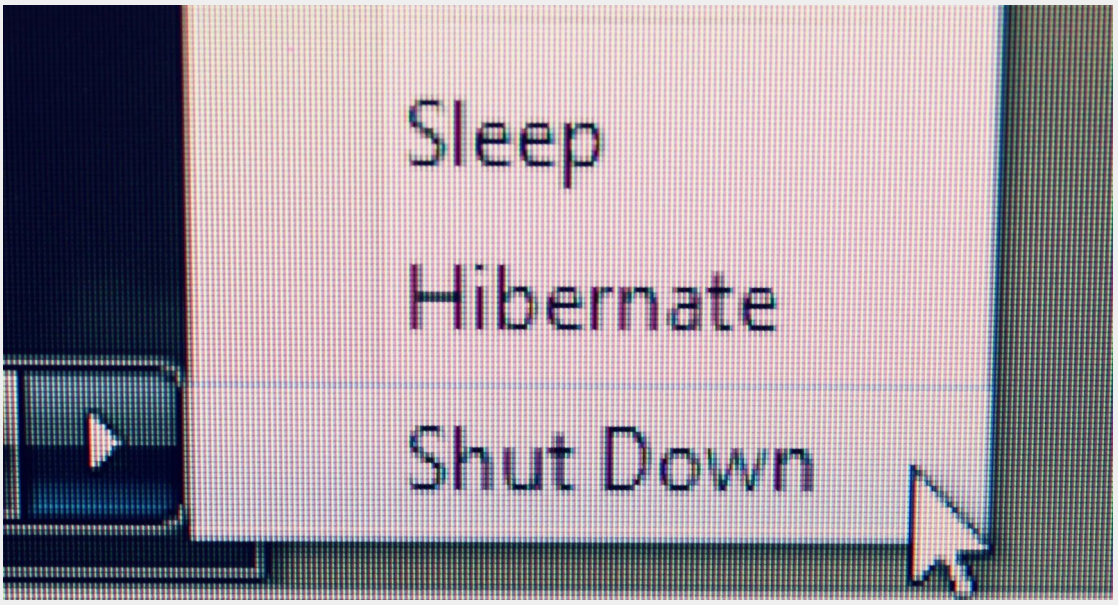


Be Careful What You Download



Downloading just any email attachments you come across can be very counterproductive.It will usually undo the work of a very vigilant and efficient Antivirus program.You should never open email attachments from people you don't know or forwarded attachments from people you know since they may also be unaware but the attachments may contain unknown malicious code.

Turn Off Your Computer



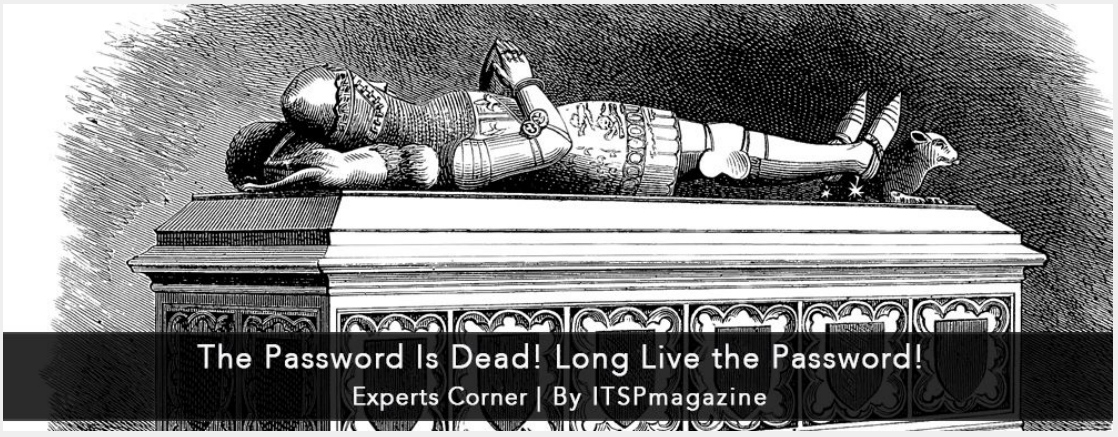
With the current high-speed internet connections(3G and 4G),many people opt to leave their computers on and ready for action.Always being 'online' or 'on' renders computer more susceptible to malicious people out there who are always looking for botnets and zombies to assist them carry out their exploits.Others might be looking for people to attack and leaving your computer on gifts them that chance,turning the computer off effectively severs an attacker's connection-Be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users(**This simple act really goes a long way to prevent Cyber Attacks**).



7]The Future OF Passwords



The Password Is Dead



A popular and recurring phrase within the computer and technology circles.The argument for this is that the replacement of passwords by a more secure means of authentication is both necessary and imminent.There is some truth to it and if the main shortcomings of passwords are not addressed it could be truly dead.The argument first sprang up about more than a decade ago,in the year 2004.*Various stakeholders and players in the world of technology such as* ***Bill Gates*** *claim that passwords are not enough to protect users.In Gates' words-->"They (passwords) just don't meet the challenge for anything you really want to secure".Most of the reasons given often include reference to the usability as well as security problems of passwords.****Jeremy Grant****,the head of the* ***NSTIC*** *Initiative (****that is the US Department of Commerce National Strategy for Trusted Identities in Cyberspace****),is quoted as declaring that "passwords are a security disaster,we want to shoot them dead".****Eric Grossed****,The VP of Security Engineering at* ***Google****,States that " passwords and simple bearer tokens,such as cookies are no longer sufficient to keep users safe".In their book, "* ***The Persistence of Passwords*** *",****Cormac Herley*** *and* ***Paul Van Oorschot*** *suggest that every effort should be made to end the " spectacularly incorrect assumption" that passwords are dead,stating that "no other single technology matches their combination of cost,immediacy and convenience" and that "passwords are themselves the best fit for many of the scenarios in which they are currently used".*In a sense I agree with them,I mean the password is quite an effective invention which fits many

scenarios and purposes,it would take quite a long time to try and phase them out and we may never even find a suitable replacement that even comes close to it.However,that doesn't mean that they haven't being efforts and initiatives to try and eliminate passwords,some I doubt are known out there in the public domain and are just used on a small-scale level at companies and corporations.Some of these initiatives include:

1) **Microsoft's Cardspace**
2) **NSTIC**
3) **Identity 2.0 Proposals**

It is worth noting that there are many alternatives being fronted as a possible and feasible replacement for passwords.However,most of them do not even come close and are worse,alternatives with a fairly high chance of success such as **Project Abacus** would still be have passwords as a fallback embedded in it's architecture;when things do not work out as expected.The password **might** still have a very vital role to play in the future.

Replacing the Password?



The numerous ways in which traditional passwords can be compromised has

prompted the development of other techniques to try and address the traditional passwords' shortcomings.This is quite in order but it should not be misinterpreted to mean that passwords are completely useless and we no longer need them,on the contrary we still have a long uphill task if we are to repeal passwords in totality as we know them and replacing them with something better or at least close to the security that passwords offer.The phrase "The Password is Dead" has only fuelled the debate that the password has 'completely failed' and must urgently be replaced.Few of the proposed alternatives are now **universally available while some still remain inadequate in practice**.In fact,Passwords are not being given much of a lifeline by majority of the experts;maybe a decade or less.

A 2012 paper by the IEEE;"The Quest To Replace Passwords",examines why passwords have proved so hard to supplant and do away with.After examining thirty representative proposed replacements with respect to security,usability and deployability that they concluded "none even retains the full set of benefits that legacy passwords already provide".



Most Popular Alternatives to Passwords

There are many techniques and means of user authentication that are now being touted as possible replacements of passwords because the end of u using passwords according to some is imminent,however,the most popular of the alternatives are:





1) **Cognitive Passwords- This technique uses question and answer cue/response pairs to verify identity.**

2) **Time-Synchronized One-Time Passwords - similar to single-use passwords in some ways,but the value to be entered is displayed on a small(generally easily pocketable) item and changes every minute or so.**

3) **Passwindow- One-Time Passwords are used as single-use passwords, but the dynamic characters to be entered are visible only when a user superimposes a unique printed visual key over a generated challenge image shown on the user's screen.**

4) **Single-use Passwords- Most users find these passwords extremely inconvenient but having passwords which are only valid once makes many potential attacks ineffective.They have however, been widely implemented in personal online banking,where they are known as Transaction Authentication Numbers (TANs).Very effective when the user has only a small number of transactions.**

5) **Biometric Method- Its based on unalterable personal characteristics.They require additional hardware scan e.g**

Fingerprints, Irises etc.In case of a Lack of the additional hardware may present a challenge.They have been proven to have high error rates and also proven far easily to spoof which is quite severe as some data cannot be replaced once compromised e.g it is not possible to change your fingerprints.There have been massive implementation of Fingerprint scanners on iPhones and Samsung Galaxy's,Iris Scanning such as Myris Scanning.A good example of biometric compromise is the Iris Scanning on Samsung's devices can be easily fooled by simply holding up a photograph of the user;a vulnerability that has prompted Samsung to request users to blink.

6) **Tokens- A unique piece of data that allows access to a website.The Illiri system sends a sound to smartphones that users then play to their computer as a means of authenticating login.Clef on the other hand,sends an image to smartphones that is shown to the computer's webcam.Tokens are however less convenient.**

7) **Non-Text based Passwords- These include graphical Passwords or mouse movement based passwords.Graphical Passwords are an alternative means of authentication for log-ins intended to be used in place of conventional(traditional)passwords; they use Images, Graphics or Colours instead of Letters,Digits and Special Characters.One such system requires users to select a series of faces as a password,utilizing the human brain's ability to recall faced easily (Butler,Rick A.Face in the** http://crowd.mpag.com
Some implementations,require the user to pick from a series of images in the correct sequence in order to gain access (similar to that of reCAPTCHA-->prove that you're not a robot),Graphical password or Graphical User Authentication (GUA) http://search security.techtarget.com.

8) **Another Graphical password solution creates a One-Time Password using a randomly generated grid of images.Each time the user is required to authenticate,they look for the images that fit their pre-chosen categories and enter the randomly generated alphanumeric character that appears in the image to form the One-Time password.Graphical passwords are promising at the moment,but are not widely used at a substantial level and scale and studies are still being done to determine their usability and implementation in the Real World.**

While it is a popular belief that graphical Passwords would be harder to

crack,I wouldn't be too sure if recent happenings are anything to go by.A famed hacker allegedly recreated,the fingerprint of the ***German Defense Minister****...from get this,a photograph!(Mindblowing),he is also alleged to have defeated* ***Apple's Thumbprint Verification*** *within 24 hours of the Launch of the iPhone 5s(Enough said...I rest my case).Graphical Passwords definitely aren't out of the woods yet,there's a really long way to go.*



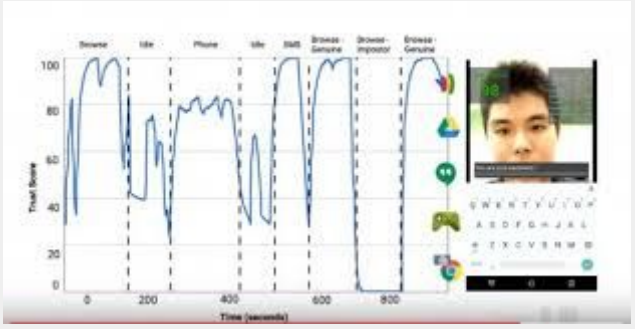
Project Abacus



*Slightly different,unique and the best alternative to passwords thus far,that it rightly deserves a mention on its own.Born from the desire to find a way to make authentication systems device-driven,rather than human driven.***Project Abacus** *first came up at Google's I/O Conference of 2015 and brought into more perspective and introduced to developers last year,Google partnered with multiple universities, as well as 25 experts from 16 institutions, to create a system which, according to* ***Google****,is now ten times more secure than fingerprint authentication;it uses Machine Intelligence that comes up with a Trust Score.Google's head of their* ***ATAP*** *(****Advanced Technology and Projects****) research unit,****Daniel Kaufman****,has said that Project Abacus opts for biometrics over two-factor authentication;the main goal being to eliminate the burden and vulnerabilities of PINs and Passwords from the user to the device.It is different from* ***Google's Smart Lock*** *system,which uses trusted locations,bluetooth and face recognition to allow you to unlock your device with a PIN or password.The basic principle behind Project Abacus is the fact that since we humans are not good at recalling PINs and Passwords,we are quite good at being ourselves.Running in the background of your device,it gets to know you,and collects data about you and your usage patterns – such*

*as typing patterns,walking patterns in relation to location,current location, speed, facial recognition and voice patterns – and uses that data to create your own,unique cumulative Trust Score.This Trust Score is fundamentally about how confident the system feels that you are who you say you are.For instance,if you set the system to allow your phone to access an account in a particular app,you can access the app without typing in a password so long as the Trust Score is above the minimum for that app,On the other hand,if the Trust Score doesn't meet the prescribed threshold then complementary mechanisms like asking for you to enter a password to access a certain App or Resource on your Phone.However,it is prudent to note that Different Apps require different level of Trust Scores i.e It makes a lot of sense to have your Bank require a higher Trust Score than a Messaging App or even a Game App.Trust API has been developed from the ideas of Project Abacus after research by Google's search and machine intelligence groups,and it started trials with high security-level systems like banks in June of 2016.It would be correct to say that Google really has big ambitious plans for Project Abacus;trials have been conducted with over 33 Universities in across 28 States of the **United States of America**.According to Google's projections,the technology would have been availed to **Android Developers** by end 2016 for subsequent implementation into Apps.The success of this Project and implementation is up to the discretion of Developers because then have to ascertain whether Project Abacus has an edge over rival company's methods and alternatives like **Apple's Touch ID**.*

Progress and Innovation is good,very good intact.However,we must get it right on the balancing act.While Google's approach with Project Abacus is quite spot on to solve some security challenges, it also poses some risks;Can we be able to trust Google to secure such vital and sensitive information about us successfully or will they be endlessly hunted down by cyber criminals?especially for data related to banks and other apps.There is also the issue that mobile phones will become 'super private',more private than they are now and maybe even inconveniencing you.Your friends will start to see you as a weirdo and uncool.This is because sharing your phone with other people might interfere and compromise data collection and you don't want that to happen.



Final Thoughts



Many famous Scholars and Thinkers such as Aristotle,Plato and Socrates had one thing in common;at some point in their lives realized that Knowledge while being good,is not really the end goal,instead applying the knowledge is the Ultimate end goal.Another Scholar Goethe famous' saying that Knowing is not enough,we must apply is simple and straightforward; imploring us to act on whatever knowledge we have to make our lives better.It would only be fair to say that we have tackled a great deal about Passwords in this ***eBook****.The onus is on us now to implement all that,especially the contents of* ***Chapter 3****.While this gives an edge or a lifeline of sorts than other people who haven't got the information that we now have,'knowing something and not living by it is dishonest',it was once said;we ought to implement what we know.We must maintain an open mind to other developments in the world of Technology.The existence of Password Crackers and the fact that other tools and inventions are being made by the day meaning we are not as safe as we would like to think,but* ***Frank A. Clark*** *said that If one can find a path with no obstacles,it probably doesn't lead anywhere.We therefore have to appreciate the strides in the computer world,albeit positive or otherwise because it means that we are improving and we are not stuck to one point.Implementing Secure Techniques whilst looking out for improvements and happenings that will impact us either positively or otherwise is the only sure path,since as I've always said throughout this* ***eBook****;****Optimum Security*** *is just an illusion,and we would only be lying to ourselves,letting our guard down and leaving ourselves vulnerable to attackers.As the Heartbleed bug and other data breaches have demonstrated,online services ought to always do things proactively and beforehand(release software patches for vulnerabilities before they are exploited) because our only security is the ability to change.They should make sure that their systems do not render our efforts useless,and that we work in tandem,if at all a* ***substantive*** *degree of* ***Cyber Security*** *is to be realized; not on paper but in reality.Keeping in mind the shortcomings of passwords there are good prospects for alternatives such as Project Abacus,but it still doesn't change the fact that we all have to work together and maintain good security practice across the board.****Can it be said that we cannot do without passwords as we know***

them?*Perhaps the fact that* ***passwords have been around since the inception of the web might have made us too comfortable with them*** *that we are not giving new alternatives any thought or chance,instead to overlook and ignore some of the flaws that come with passwords however serious they might be.When it comes to the bigger picture that is* ***Cyber Security****,passwords might actually be the grey area,and there are so* ***many dynamics*** *to look into and the security challenges encountered today are not of the 90's when the web was just a new kid on the block,technology and innovation has changed a lot and we have to adapt if we are to survive and resolve the prevailing issues but I feel that firstly,we have to understand the role and place of passwords today.****Are Passwords Guised Indispensables' or Liabilities?***

About the Author

Kelvin Karanja is a Computer Science ,Technology enthusiast and Innovator.He is fascinated by Technology be it something to do with Computers:Software,Programming and Hardware,Other Gadgets and Digital Machines,the IoT and emerging technology trends.He is especially interested in the Computer Security Discipline; carrying out a lot of studies and research.He believes that the Modern Computer Era,propelled by such studies,research and innovation by like minded people could overcome the many challenges and impact people positively and go down the annals of history as the best age for mankind in terms of Computers and Technology.He is a firm believer in the Norman Cousin's famous saying,'Optimism doesn't wait on facts.It deals with prospects.Pessimism is a waste of time'.You can find him on Twitter:

- **KevoKaras@kevokaras(https://twitter.com/KevoKaras)-Personal Account as he tweets the tech!**
- **Tech Bytes@TBytes(https://twitter.com/TBytes)-An account solely dedicated to talk about technology,science and innovation.**
- **Also feel fell to ask any question,comment or suggestions etc by Sending an email to: techbyteske@gmail.com**